INFORMATION WARFARE

Legal, Regulatory, Policy and Organizational Considerations for Assurance

4 July 1995

"The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced US technologies provide our forces."

[Joint Pub 1]

A Research Report for the:
Chief, Information Warfare Division (J6K)
Command, Control, Communications and Computer
Systems Directorate
Joint Staff
The Pentagon
Washington, DC 20301

INFORMATION WARFARE

Legal, Regulatory, Policy and Organizational Considerations
for
Assurance

4 July 1995

"The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced US technologies provide our forces."

[Joint Pub 1]

A Research Report for the:
Chief, Information Warfare Division (J6K)
Command, Control, Communications and Computer
Systems Directorate
Joint Staff
The Pentagon
Washington, DC 20301

INFORMATION WARFARE

Legal, Regulatory, Policy and Organizational Considerations
for
Assurance

4 July 1995

A Research Report for the:
Chief, Information Warfare Division (J6K)
Command, Control, Communications and Computer
Systems Directorate
Joint Staff
The Pentagon
Washington, DC 20301

Prepared by:
Science Applications International Corporation (SAIC)
Telecommunications and Networking Systems Operation
Contract No. MDA903-93-D-0019

THE JOINT STAFF
WASHINGTON, DC

3 July 95

Support to the warfighter in the information age poses significant challenges for the Department of Defense and the nation. The current information infrastructure, while embracing the advantages offered by information-based technologies, must respond to the significant vulnerabilities inherent in its systems. While some activities are under way to address information assurance needs, more work is needed to advance this national security issue of growing urgency and importance.

In recognition of this need, I commissioned a study to identify and document current organizational and legal conditions as an early step in the formulation of an information protection strategy. This document represents the results of that effort. The focus is on establishing a baseline to identify the participants and illuminate key considerations.

This product is solely a research effort. Any judgments expressed or implied are those of the study group and should not be interpreted as official Joint Staff positions.

We would be grateful for feedback regarding this product. If you have any questions or comments regarding this report, please call my Director of Information Warfare, CAPT William Gravell, 703-614-2918, or his lead action officer for this effort, Major Steve Spano, at 703-697-1199.

AK Cebrowski

ARTHUR K. CEBROWSKI
Vice Admiral, USN
Director for Command, Control,
Communications and Computer
Systems

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

PREFACE

Performing essential national security-related functional activities is depending more and more on a rapidly evolving, supporting information infrastructure. In view of the dependency, and because the Department of Defense (DoD) information infrastructure is embedded in larger national and international infrastructures, DoD officials, their advisors, and others within and outside the government have recommended to the National Security Council staff that it may be necessary to initiate interdepartmental/interagency discussions. Topics of such a dialogue would include the dependency and vulnerability issues and the need for national policy to deal with them. The Chief, Information Warfare Division (J6K), Directorate of Command, Control, Communications, and Computer Systems (J6), the Joint Staff, commissioned this report to prepare the Joint Staff to participate in and contribute to these discussions.

The breadth and extreme complexity of the subject matter, other related ongoing activities, and the scope of the task limited the number of environmental areas and organizations which could be addressed. The report does, however, address the breadth and complexity of the policy and strategy issues and summarize the views of those in positions of importance to the development of policy for information warfare.

To develop the organizational policy considerations, the study group reviewed organizations which have a stated role in information warfare and organizations which have related missions and functions. This report presents several key organizations in a broad range encompassing international, national, state and local, public and private, government and industry organizations.

The environmental areas examined were:

- Information Infrastructure
- Legal Environment
- Regulatory Environment
- Policy Environment
- Emerging Technologies
- Adversary Capabilities.

Because of the extensive organizational and reference information documented herein, this report should also be viewed as a source book on information warfare/information assurance background, stakeholders, interests, and activities.

The report is organized as follows:

- Section 1 introduces the report and provides context.

- Section 2 addresses each of the environmental areas noted above.

- Section 3 discusses the methodology of the organizational reviews and provides key findings.

- Section 4 summarizes the policy and strategy issues.

- Appendix A summarizes organizations which have missions and functions which may relate to defensive information warfare/information assurance. The first page of Appendix A contains an index to the organizations considered in the report. Each organizational summary identifies:

    - The organization
    - A senior information official
    - Points of contact
    - Information warfare/information assurance related missions and functions
    - Information warfare/information assurance activities, issues, best practices, and lessons learned.

  Each summary also includes a chart that shows the organizational entities which conduct related activities. A consolidated list of points of contact with telephone numbers is found at the end of each major section in Appendix A.

- Appendix B includes an annotated bibliography of applicable U.S. Code, regulatory documents, policy documents, and periodical articles, and, additional references without annotations.

- Appendix C lists the acronyms used throughout the report.

A summary version of this report contains the Preface, Sections 1 through 4, and Appendix C, Acronyms. The summary version includes a PC-compatible disk which contains Appendices A and B. The electronic Appendix A contains an organization chart in Microsoft Excel format showing all of the organizations summarized in Appendix A of the complete version of the report. This organization chart features, for most organizations, information buttons which, when selected, show the viewer the organizational summaries. The disk also includes the points of contact listings found in Appendix A. The electronic Appendix B is a Microsoft Word document.

Information in this document is current as of 30 June 1995.

SECTION 1

INTRODUCTION

The national security posture of the United States is depending more and more on the U.S. information infrastructure and the larger Global Information Infrastructure (GII). These information infrastructures (which consist of information, information systems, telecommunications, networks, and technology) depend, in turn, upon other infrastructures such as electrical power and energy. Over 95 percent of the worldwide telecommunications needs of the Department of Defense (DoD) are satisfied by commercial telecommunications carriers.

These information infrastructures are very vulnerable. Within the last two years, electronic intruders have penetrated major U.S. telecommunications carriers and Internet service providers, many international Post, Telegraph, and Telephone organizations, and a wide variety of end-user systems. These intruders have included foreign intelligence agents, economic espionage agents, organized crime members, drug cartel members, private detectives, hackers, and insiders.

In recognition of the growing dependency on a vulnerable information infrastructure over which they have little control, DoD officials, advisory committees, and others have recommended to the National Security Council (NSC) staff that it may be necessary to initiate Federal Government interdepartmental discussions of the dependency and vulnerability issues and the possible need for national-level policy to deal with the issues.

The Information Warfare Division (J6K), Directorate of Command, Control, Communications, and Computer Systems (J6), the Joint Staff, commissioned this report to prepare the Joint Staff to participate in and contribute to these discussions.

The lack of a common understanding of terms and definitions limits the ability of the stakeholders to conduct meaningful discussions about the information environment. This report uses the term *information warfare* in the broadest sense to encompass all offensive information warfare and defensive information warfare actions. The term *defensive information warfare* includes all actions to ensure the availability, confidentiality, and integrity of reliable information vital to national security needs. The term *information assurance* denotes the availability and integrity of information and, for the purpose of this report, is synonymous with defensive information warfare. In general, the term *information warfare* is used when discussing organizations and activities within the DoD. The term *information assurance* is used when discussing other organizations and activities. The use of the terms *senior information warfare official* and *senior information assurance official* does not imply that there are officially designated positions bearing these titles. These terms indicate a senior official within the organization who has been or might conceivably be assigned the responsibilities for information assurance.

1.1 PURPOSE

This report documents various organizational and environmental considerations which may influence the formulation of information warfare policy and strategy.

1.2 SCOPE

To develop the organizational considerations, the study group reviewed organizations which have a stated role in information warfare or information assurance and organizations which have related missions and functions. The review consisted of research and interviews to identify organizational structures, organizational interests, key individuals (stakeholders) within the organizations, information warfare-related practices, lessons learned, and issues. Figure 1-2-1 shows the types of organizations reviewed.

- ***International***
- ***National***
  - **Public**
    - **Academia**
    - **Public Interest Groups**
  - **Private**
    - **Industries**
    - **Associations**
    - **Alliances**
- ***Federal Government***
  - **Executive Branch**
    - **Department of Defense**
    - **Other Departments**
    - **Interagency Groups**
    - **Advisory Committees**
  - **Independent Establishments and Government Corporations**
  - **Legislative Branch**
  - **Judicial Branch**
- ***State and Local Governments***

Figure 1-2-1. Types of Organizations Reviewed

This report presents several key organizations in this broad range. Because of Joint Staff familiarity with DoD activities, this document emphasizes departments other than the DoD and agencies categorized as Independent Government Establishments and Corporations (such as the National Aeronautics and Space Administration (NASA) and the General Services Administration (GSA)).

Figure 1-2-2 shows the environmental areas examined for policy and strategy considerations.

- Information Infrastructure
- Legal Environment
- Regulatory Environment
- Policy Environment
- Emerging Technologies
- Adversary Capabilities

Figure 1-2-2. Environmental Areas

These areas complement ongoing DoD activities that explore other environmental aspects such as requirements, doctrine, training and education, research and development, test and evaluation, and acquisition. Also, at the Federal Government interdepartmental level, discussions of information warfare/information assurance issues and the possible need for a national-level policy would center around these environmental areas.

Because of the general responsibilities of the Information Warfare Division of the Joint Staff, this report deals primarily with defensive information warfare issues.

1.3 BACKGROUND

As shown in Figure 1-3-1, Joint Pub 1 advocates the exploitation of the "information differential" in the joint campaign. In exploiting that differential, joint warfighters will depend increasingly upon information and information systems in both offensive and defensive operations. From a defensive information warfare perspective, various individuals, organizations, special studies, and advisory committees have raised concerns regarding the growing dependence of national security upon a vulnerable information infrastructure.

> "The Joint Campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situations which advanced U.S. technologies provide our forces."

Figure 1-3-1. Joint Pub 1 Quote

During the previous three decades, when automated data processing was primarily confined to mainframe computers operating in physically secure facilities, the Congress attempted to define responsibilities of Federal Government organizations and officials for the protection and privacy of information. These attempts notably improved the fields of computer security (COMPUSEC), communications security (COMSEC), and information systems security (INFOSEC) in protecting information and the privacy of individuals.

Still, responsibilities for the protection of the information infrastructure and the privacy of the information contained in the infrastructure have not been well defined. Most of the legislative requirements for the protection and privacy of information apply only to the Federal Government.

During this same period, the successful performance of essential economic and national security-related functions became more and more dependent on automated information systems. Banking, retail, telecommunications, and other industries automated operations for cost, competitive, and other reasons. Government and military organizations automated key functional activities to improve response times, save costs, and better meet perceived threats.

Within the last decade, personal computers, workstations, data bases, and mainframes have been interconnected into distributed information networks. This interconnection is continuing at an ever increasing rate. (For example, the Internet now adds a new network every 30 minutes!) Through the Internet and other data networks, government networks are interconnected with commercial networks, which are interconnected with military networks, which are interconnected with financial networks, which are interconnected with the networks which control the distribution of electrical power, and so on. It is now almost impossible to distinguish where one network ends and another begins in this extensive and complex information infrastructure.

This report identifies some of the complexity and key considerations that affect the development of policy regarding the exploitation and protection of the information infrastructure.

SECTION 2

ENVIRONMENTAL CONSIDERATIONS

This section discusses the environmental areas.

Section 2.1 discusses the complex nature of functional activities and the underlying information infrastructure upon which they depend. It discusses the nature of the information infrastructure, its vulnerabilities, and some of the ongoing activities to improve the reliability of the infrastructure.

Sections 2.2, 2.3, and 2.4 discuss the legal, regulatory, and policy environments and focus on those laws, regulations, and policies which are most relevant to information warfare/information assurance, in particular, those that identify key roles, functions and responsibilities. *Public law* applies to all U.S. citizens. It forms the capstone documentation which defines organizations and their responsibilities and which bounds their information warfare/information assurance-related activities. *Regulations* have the full force and effect of law, are associated with permanence, and apply to all U.S. citizens. *Policy* generally applies to some subset of the population and may change with administrations.

Section 2.5 discusses emerging technologies in the communications and information security fields.

Section 2.6 discusses the potential adversary capabilities and poses related questions and challenges for the intelligence community.

This page intentionally left blank.

2.1 INFORMATION INFRASTRUCTURE

2.1.1 Introduction

This section discusses the complex nature and interdependencies of functional activities and the information infrastructure (to include the telecommunications networks) which serves as the foundation of the activities. It discusses the nature of the information infrastructure, its vulnerabilities, and some of the ongoing activities to improve the reliability of the infrastructure.

2.1.2 Functional Activities and the Information Infrastructure

The production and delivery of goods and services directly affects the national and economic security of the U.S. and directly influences the readiness of the military forces. The delivery of these goods and services depends on the complex interactions of various functional activities, industries, commodities, and political, economic, and social conditions. Figure 2-1-1 illustrates some components of national and economic security and their possible interactions and interdependencies. The relationship of the shaded areas is discussed in the text following the figure.

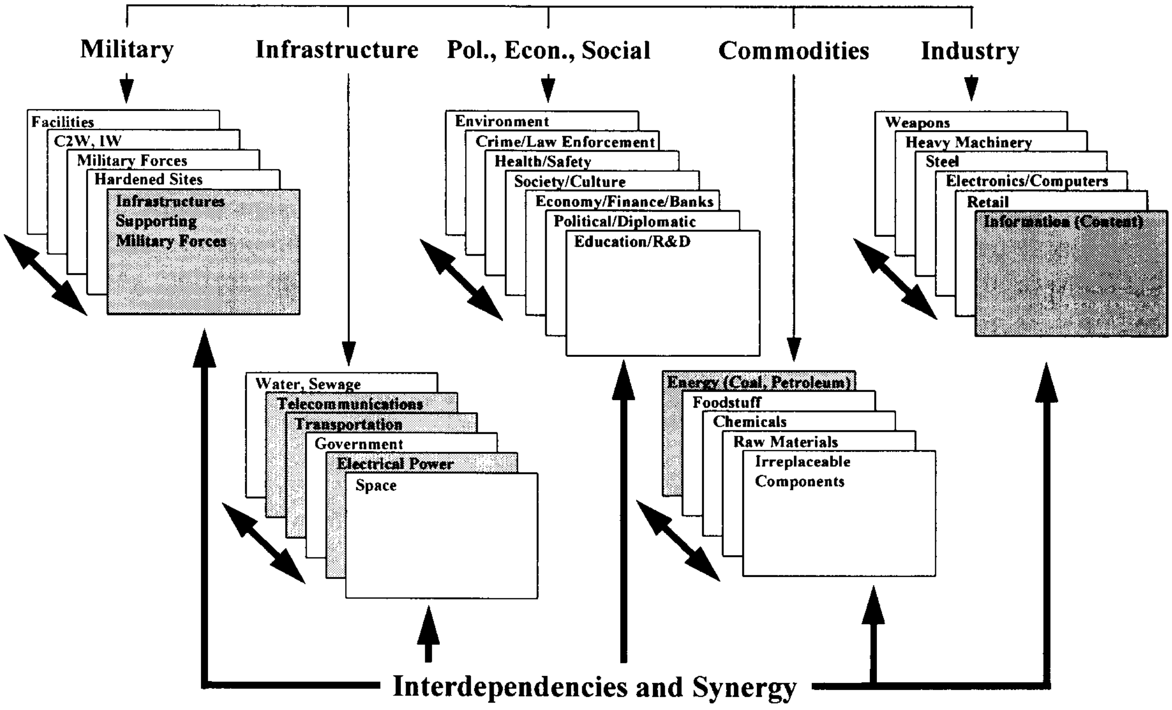


Figure 2-1-1. Components of National and Economic Security

Consider, for example, the functional activity of deploying a military force from the United States to deal with a regional crisis. This deployment requires moving individual units to ports of debarkation, transporting those units to the region of interest, and employing the force to deal with the crisis. If this deployment involves a sizable force, these activities depend on the use of the Nation's transportation infrastructure. Coordinating the activities depends on an effective telecommunications infrastructure. Both the transportation and telecommunications infrastructures depend on the availability of electrical power, which, in turn, depends on the availability of sufficient energy sources to produce the needed electrical power. Coordinating transportation activities and providing electrical power also depend on an effective telecommunications infrastructure.

Most functional activities use the information infrastructure, and in particular the telecommunications networks. In the private sector, these activities include such actions as governing, banking, and manufacturing in the private sector. In the military environment, these activities might include transportation, logistics, pay and other monetary disbursements, manpower and personnel, and training. The information infrastructure supports all of these activities, and it is difficult to distinguish which portions of the infrastructure support which functional activities. Therefore, this discussion will address the general nature of a singular, total information infrastructure, its vulnerabilities, and some of the activities under way to improve the reliability of the infrastructure.

2.1.3 Nature of the Information Infrastructure

The information infrastructure is extremely complex. There is no simple way to define it, to establish its bounds, to measure its impact, or to identify clear responsibilities for the evolution, operation, maintenance, and repair of the infrastructure. Therefore, the various views of the infrastructure presented by this report only partially address the complexity.

One way of viewing the information infrastructure is in terms of its basic components. In very simple terms, the information infrastructure comprises of the components necessary for the transportation of information, the information itself, the means for creating, gathering, and processing data to obtain information, and the storage of the data and information. In the broadest sense, the infrastructure consists of data, information, equipment, facilities, telecommunications, and people. Table 2-1-1 provides examples of typical information infrastructure components.

Table 2-1-1. Typical Information Infrastructure Components

- **Scanners**
- **Keyboards**
- **Telephones**
- **Fax Machines**
- **Computers**
- **Switches**
- **Compact Disks**
- **Video and Audio Tape**
- **Facilities**
- **Meteorological Data**
- **Weather Information**
- **Cable**
- **Wire**
- **Satellites**
- **Optical Fiber**
- **Microwave Nets**
- **Television**
- **Monitors**
- **Printers**
- **People**
- **Information Content**
- **Cameras**

Another way of viewing the information infrastructure is as a collection of various networks and services. Some of these networks and services, such as the Internet and the public telephone and public data networks, have an identity of their own and are clearly an integral part of the information infrastructure. Others, such as the financial networks and services, have developed within a specific industry and have evolved into a complex internetwork necessary to provide responsive support to the customer. Table 2-1-2 shows some of these networks and services.

Table 2-1-2. Typical Information Infrastructure Networks and Services

- **Internet**
- **Public Switched Telephone Network**
- **Public Data Networks**
- **Cellular Networks**
- **Commercial Satellite Networks**
- **Broadcast Radio Networks**
- **Broadcast TV Networks**
- **Cable TV Networks**
- **Defense Data Network**
- **Direct Broadcast Satellite (TV)**
- **On-line Services**
- **Publishing Services**
- **Entertainment Services**
- **Financial Networks and Services**
- **Power Networks**
- **Transportation Networks**
- **Public Safety Networks**
- **FTS2000**

The information infrastructure can also be thought of in terms of the various domains it serves. Table 2-1-3 shows some of these domains. In reviewing the table, it should be evident that the infrastructure contains a vast amount of sensitive information.

Table 2-1-3. Typical Information Infrastructure Domains

- **News**
- **Health and Safety**
- **Navigation**
- **Weather**
- **Government**
- **Transportation**
- **Entertainment**
- **Intelligence**
- **Military**
- **Law Enforcement**

The information infrastructure should also be considered in terms of the stakeholders with an interest in the future evolution of infrastructure. Table 2-1-4 shows some typical stakeholders. The military prefers an extremely reliable and robust infrastructure to ensure the availability of critical information during times of crisis. U.S. citizens insist on protection of their individual rights, particularly the right to privacy. On the other hand, sellers of information content insist on universal service so that their market is larger.

Table 2-1-4. Typical Information Infrastructure Stakeholders

- **Federal Government**
- **Military**
- **The Economic Marketplace**
- **Industries**
- **Industry Alliances**
- **Congress**
- **State Governments**
- **Regional Governmental Alliances**
- **Public Servants**
- **Academia**
- **International Economic Groups**
- **International Political Groups**
- **Labor Organizations**
- **Local Governments**
- **Public Interest Groups**

The infrastructure will be shaped by the interests of these stakeholders. For example, the Federal Government may seek to intervene in the evolution of the infrastructure for national security and other considerations. Table 2-1-5 shows some of the typical stakeholder interests which may be unique to individual stakeholders or shared by groups of stakeholders.

Table 2-1-5. Typical Information Infrastructure Stakeholder Interests

- **Universal Service**
- **Information Assurance**
- **Intellectual Property Rights**
- **Interconnection**
- **Interoperability**
- **Ownership**
- **Pricing**
- **Jobs**
- **Regulation**
- **Privacy (Security)**
- **Spectrum Management**
- **Standards and Protocols**
- **Technologies**
- **User Education about Vulnerabilities**
- **User Friendly Interfaces**

It should be clear by now that there is no single view of the information infrastructure, nor is there a simple way of understanding its complexity. The evolution of the infrastructure (past, present, and future) was, is being, and will be formed by a multitude of competing interests and technologies. Access to the infrastructure is essentially unlimited. Access to the information located throughout the infrastructure is not well controlled. Even when access is controlled, it is not well managed. For example, recent tests by the Defense Information Systems Agency (DISA) on logistics and medical systems revealed that 88 percent of targeted computers could be penetrated, only 4 percent of the successful penetrations were detected, and only 5 percent of the detections were reported.

2.1.4 Information Infrastructure Vulnerabilities

The infrastructure is vulnerable to many disruptive forces including natural events, mistakes, technical failures, and malicious acts:

- A lightning strike on a critical node in a network may cause node failure; an earthquake or hurricane may only physically disrupt the network but also cause network congestion, another source of disruption.
- Inadvertently erasing a data base containing terrain data critically needed for a cruise missile strike may compromise a key part of an offensive strike.
- Cutting a fiber optic cable with a backhoe may result in the loss of a primary telecommunications link.
- Power failure at a critical network node may cause a significant loss of data and information and may isolate portions of the network.
- Corruption of key network management data by a network manager can cause many networks to fail.
- Viruses introduced by an enemy agent located in a safe haven can cause a network to become overloaded and ineffective or to break down at a critical juncture.

The disruptive nature of such occurrences, whether maliciously or unintentionally caused, was demonstrated in 1988, when a software worm was released into the Internet infecting over 6000 host computers worldwide in less than two hours, and in 1991, when the near-total shutdown of telephone service in the Baltimore-Washington area was caused by a one-byte coding error—a "d" was replaced with a "6."

Over the past two years, unknown intruders have penetrated major U.S. telecommunications carriers, major Internet service providers, many international Post, Telegraph, and Telephone entities, and a wide variety of end-user systems. Targets of these intrusions have included those shown in Table 2-1-6.

Table 2-1-6. Targets of Intrusions

- **Service Control Points**
- **Signal Transfer Points**
- **Network Elements**
- **Network Element Managers**
- **X.400 Gateway Systems**
- **Billing Systems**
- **Provisioning Systems**
- **Loop Maintenance Systems**
- **Document Support Systems**
- **X.25 Packet Data Networks**
- **Digital Cross Connect System**
- **Research and Development Systems**

Given the extreme dependence of our national and economic security upon the information infrastructure, it is prudent to assume that the infrastructure will be the target of an information warfare attack. Section 2.6 discusses the adversaries who might conduct such attacks. These attacks may take several different forms:

- Physical attacks on infrastructure components such as computers, communications, software, data, cables, and the control process.
- Physical attacks on infrastructure support such as buildings, power, and environmental control units.

- Physical attacks on or subversion of operating and support personnel.
- Logic attacks on infrastructure components.
- Logic attacks on computer-controlled environmental control units.
- Combined physical and logical attacks to mask one or the other.
- Logic attacks on data (destruction or disruption).

If the infrastructure is directly attacked, it is not known which portions of the infrastructure will be affected, or what effect the loss of portions of the infrastructure will have on the performance of essential functional activities. These areas will require extensive study and research.

2.1.5 Activities to Improve Infrastructure Reliability

There are a number of ongoing activities intended to improve the reliability of the information infrastructure. Describing all of these activities in detail is not within the scope of this report. The following paragraphs provide a sampling of these activities from a DoD, a Federal Government, and a national-level perspective.

Several offices within the Office of the Secretary of Defense (OSD) and the Joint Staff are assessing infrastructure reliability, including net assessments, policy reviews, assessments of current and planned programs, and a National Defense Infrastructures Survivability Study.

Among the Defense Agencies, DISA is primarily responsible for protecting the DoD portion of the information infrastructure. DISA has published documents related to the protection of the infrastructure and is currently expanding its Defensive Information Warfare (DIW) Management Plan to include related Service and Agency plans. The National Security Agency (NSA) has research and development activities under way in the area of INFOSEC. The Advanced Research Projects Agency (ARPA) has recently established two primary research areas—one in the DIW area and one in the INFOSEC area. These ARPA research activities will deal with selected information infrastructure vulnerability and reliability issues and, to the extent possible, will be conducted on a cooperative basis with industry.

From a Federal Government perspective, Presidential Decision Directive (PDD) 29, signed in the latter part of 1994, created the Security Policy Board, which will address a variety of security issues to include information systems security and risk management. The Security Policy Board will consider, coordinate, and recommend for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices. The Security Policy Board will be the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State. This Board will coordinate the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements. In coordinating security policy, procedures and practices, the Policy Board will ensure that all U.S. Departments and Agencies affected by such decisions are allowed to comment on such proposals.

PDD 29 also established a Security Policy Advisory Board to serve as an independent, non-governmental advisory body. Five members, including a Chairman, will be appointed by the President for terms of up to three years. The Chairman will report annually to the President through the Assistant to the President for National Security Affairs on the implementation of the four policy principles, as shown in Figure 2-1-2. The Security Policy Advisory Board will also provide a non-governmental and public interest perspective on security policy initiatives to the Security Policy Board and the intelligence community.

Figure 2-1-2 also shows membership and organization of the Board. Acronyms used in this and subsequent figures are spelled out in Appendix C.

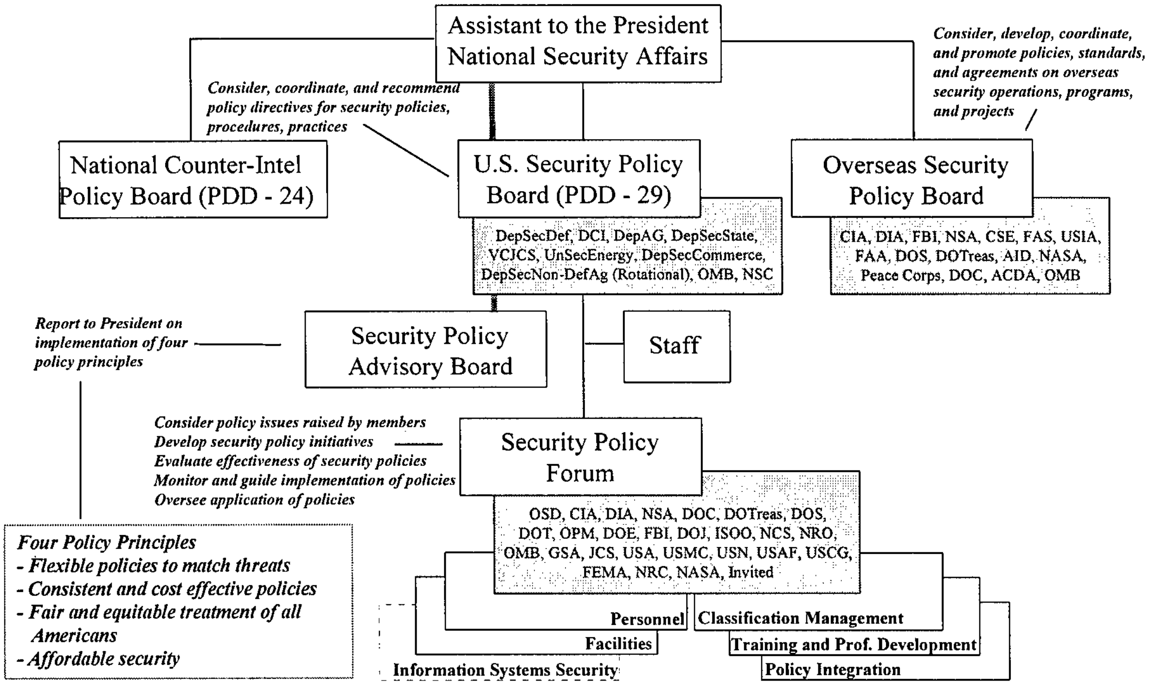

Assistant to the President
National Security Affairs
Consider, coordinate, and recommend policy directives for security policies, procedures, practices
Consider, develop, coordinate, and promote policies, standards, and agreements on overseas security operations, programs, and projects
National Counter-Intel Policy Board (PDD - 24)
U.S. Security Policy Board (PDD - 29)
Overseas Security Policy Board
DepSecDef, DCI, DepAG, DepSecState, VCJCS, UnSecEnergy, DepSecCommerce, DepSecNon-DefAg (Rotational), OMB, NSC
CIA, DIA, FBI, NSA, CSE, FAS, USIA, FAA, DOS, DOTreas, AID, NASA, Peace Corps, DOC, ACDA, OMB
Report to President on implementation of four policy principles
Security Policy Advisory Board
Staff
Consider policy issues raised by members
Develop security policy initiatives
Evaluate effectiveness of security policies
Monitor and guide implementation of policies
Oversee application of policies
Security Policy Forum
OSD, CIA, DIA, NSA, DOC, DOTreas, DOS, DOT, OPM, DOE, FBI, DOJ, ISOO, NCS, NRO, OMB, GSA, JCS, USA, USMC, USN, USAF, USCG, FEMA, NRC, NASA, Invited
Four Policy Principles
- Flexible policies to match threats
- Consistent and cost effective policies
- Fair and equitable treatment of all Americans
- Affordable security
Personnel
Facilities
Information Systems Security
Classification Management
Training and Prof. Development
Policy Integration

Figure 2-1-2. U.S. Security Policy Board

One aspect of enhancing protection is sharing information about the nature of attacks experienced by portions of the infrastructure and conducting an open dialog about related security issues. Two ongoing activities at the national level are facilitating this sharing of information and discussion of the issues. The National Communications System (NCS) and the President's National Security Telecommunications Advisory Committee (NSTAC) have been dealing with the issue of infrastructure reliability and security for several years. (Appendix A provides details of each of the organizations.) These organizations have a unique process that enables telecommunications and information industry members to share sensitive, competitive information regarding security issues without violating antitrust restrictions. This process, based on extensive non-disclosure agreements and a hierarchy of information sensitivity, also allows government and industry to share similar information. Figure 2-1-3 illustrates the entities that were created to facilitate this sharing of information.

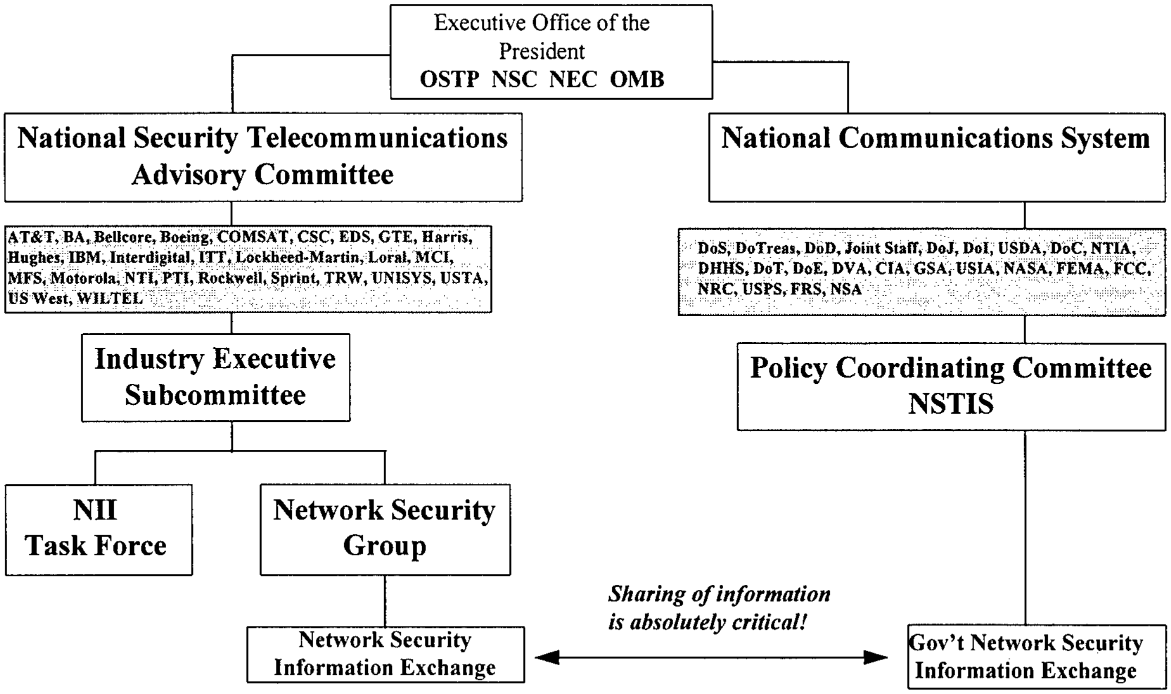

Executive Office of the President
OSTP NSC NEC OMB
National Security Telecommunications Advisory Committee
National Communications System
AT&T, BA, Bellcore, Boeing, COMSAT, CSC, EDS, GTE, Harris, Hughes, IBM, Interdigital, ITT, Lockheed-Martin, Loral, MCI, MFS, Motorola, NTI, PTI, Rockwell, Sprint, TRW, UNISYS, USTA, US West, WILTEL
DoS, DoTreas, DoD, Joint Staff, DoJ, DoI, USDA, DoC, NTIA, DHHS, DoT, DoE, DVA, CIA, GSA, USIA, NASA, FEMA, FCC, NRC, USPS, FRS, NSA
Industry Executive Subcommittee
Policy Coordinating Committee NSTIS
NII Task Force
Network Security Group
Sharing of information is absolutely critical!
Network Security Information Exchange
Gov't Network Security Information Exchange

Figure 2-1-3. NSTAC-NCS Model for Sharing Sensitive Information

The second national level activity oriented on infrastructure reliability and security is the Information Infrastructure Task Force (IITF) (shown in Figure 2-1-4), which was created by the President in 1993. (Appendix A contains the details of the task force, its subordinate committees, and its working groups.) Entities specifically dealing with reliability and security issues are the Reliability and Vulnerability Working Group (RVWG), the Government Information Technology Services Working Group, and the Security Issues Forum, which was created because of the number of security issues being raised by the IITF. The Security Issues Forum released its report, *NII Security: The Federal Role*, which is summarized in Appendix B, Policy section. With the exception of the RVWG, these entities have focused on privacy and intellectual property rights issues, not on network reliability and information availability issues.

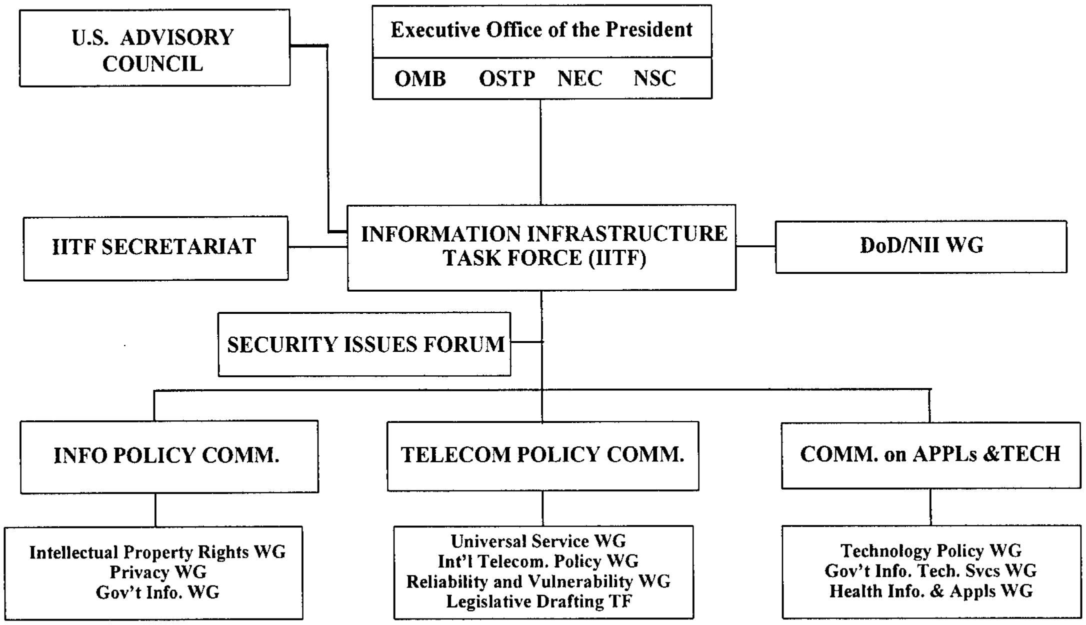


Figure 2-1-4. Information Infrastructure Task Force, Committees and Working Groups

In spite of these DoD, Federal Government, and national-level activities, and other numerous and diverse activities, some key areas remain unaddressed. One such area is the significant difference between infrastructure design and system design. System design assumes working components. However, the infrastructure is expected to function in the presence of failed components, systems, and networks; disruptions in timing; and other disruptive forces. There is no research being devoted to infrastructure design. During crises, the demand for information will increase; the infrastructure capacity will decrease. There is no mechanism in place to determine the priority of information requirements and delivery during such a crisis.

As mentioned earlier, this discussion is not intended to be exhaustive. The list of references contained in Appendix B provides additional insights into these and other related issues.

This page intentionally left blank.

2.2 LEGAL ENVIRONMENT

2.2.1 Introduction

This section reviews key parts of the U.S. Constitution and the U.S. Code that are applicable to information warfare. It also identifies assigned roles and responsibilities, and statutes which bound information warfare/information assurance activities. It discusses the implications of international law and agreements.

Legislation is signed into law to accomplish certain objectives. This report uses four recurring objectives which relate to information warfare to focus the discussion of the United States Code. The following narrative takes the reader on a legal *walk around the block*, without attempting to interpret the more complex legal issues. It takes years of review and interpretation in precedent-setting cases for public law to become specific. Even so, unique aspects of a case or changes in the environment such as new technology can result in new interpretations of longstanding law. For brevity, little attention is given to case law or to legal issues which do not generally apply to DoD. Except as otherwise noted, references to an Act include the cited Act as amended by subsequent legislation.

2.2.2 U.S. Constitution

The U.S. Constitution establishes the structure of the U.S. Federal Government and delegates the authority of the Federal Government to act in particular instances. The Bill of Rights defines certain protected rights. In defining structure and rights, bounds on government activities and broad responsibilities can be interpreted in the context of information warfare.

Bounds. The First Amendment guarantees free speech. It limits the authority of the Federal and state governments from restricting the rights of citizens to express themselves. The Fourth Amendment protects citizens from unreasonable governmental searches or seizures and limits the authority of the government to engage in surveillance of U.S. citizens or others who are physically located in the United States or whose property may be located in this country. The Ninth Amendment sets out the principle that the government is one of many delegated powers, that individuals (or state governments) retain autonomy, and that any power not delegated to the Federal government is reserved. The Fifth and Fourteenth Amendments establish the proposition that an individual may not be deprived of life, liberty, or property except by "due process of law." According to the Office of Technology Assessment in a 1993 report, the U.S. Supreme Court has also found privacy implications in other provisions of the Third, Fifth, and Fourteenth Constitutional Amendments. These amendments are shown in Figure 2-2-1.

AMENDMENT 1 Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

AMENDMENT 3 No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

AMENDMENT 4 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

AMENDMENT 5 No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence [sic] to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

AMENDMENT 9 The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

AMENDMENT 14 Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

[Amendments 1 through 10 make up the Bill of Rights, ratified in 1791. Amendment 14 was ratified in 1868.]

Figure 2-2-1. Constitutional Amendments with Privacy Implications

Responsibilities. In addition to ensuring citizens' rights, the Constitution charges Congress with providing for "the common defense and general Welfare of the United States," and the following additional responsibilities which are relevant to information warfare:

- "...securing for limited Times to Authors and Inventors exclusive Right to their respective Writings and Discoveries";
- "To define and punish ... Offences [sic] against the law of Nations";
- "To declare War";
- "To regulate interstate and foreign commerce";
- "To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."

The Constitution provides more general roles and responsibilities to the Executive and Judicial Branches. It vests all executive powers in the President and appoints him the Commander-in-Chief of the Armed Forces. The Judicial Branch, responsible for all cases "arising under this Constitution, the Laws of the United States, and Treaties made" balances the authority of the Legislative and Executive Branches. Moreover, the Judiciary has assumed the role of determining whether acts of Congress and the Executive violate the terms of the Constitution.

Constitutionally assigned responsibilities to the three branches of the Federal Government serve to check and balance authority, ensure stability, and prevent the autocracy of a single branch of government or point of view. In the Constitution, we see the genesis of one of the more controversial issues related to information warfare, the conflict between a citizen's right to privacy—his right to be left alone—and the responsibility of the government to provide for the welfare and common good and ensure economic and national security.

2.2.3 Public Law—U.S. Code

The legislative process is not well understood by many and difficult to follow for those without understanding and access. Legislation originates in the subcommittees and committees of Congress or is proposed by the Administration for consideration by Congress. On significant issues, several bills may be considered and combined. Amendments are frequently offered after a bill reaches the floor of the House or Senate. Joint committees may be formed to resolve differences between bills approved by the two houses of Congress. It is often difficult to monitor the progress of a bill, as it may languish and die in committee or be quickly passed on the eve of recess or adjournment. It is even more difficult to monitor legislation related to information warfare (IW) because of its technological and political complexity. Legislation which does not overtly apply to the DoD may still affect DoD's IW activities. It is important that Legislative Liaison Officers understand IW issues and advise policy makers on significant legislative activity. This section may serve as a useful first step in that effort.

Each statute of the U.S. Code was drafted, passed, and signed in the hope of achieving certain goals and objectives. This section describes how key statutes apply to the following information warfare related objectives:

- Protecting Individual Privacy and Providing Access to Government Information.
- Securing Federal Information and Information Systems.
- Ensuring Infrastructure Availability and Reliability.
- Defining the Criminality of Computer Fraud and Abuse.

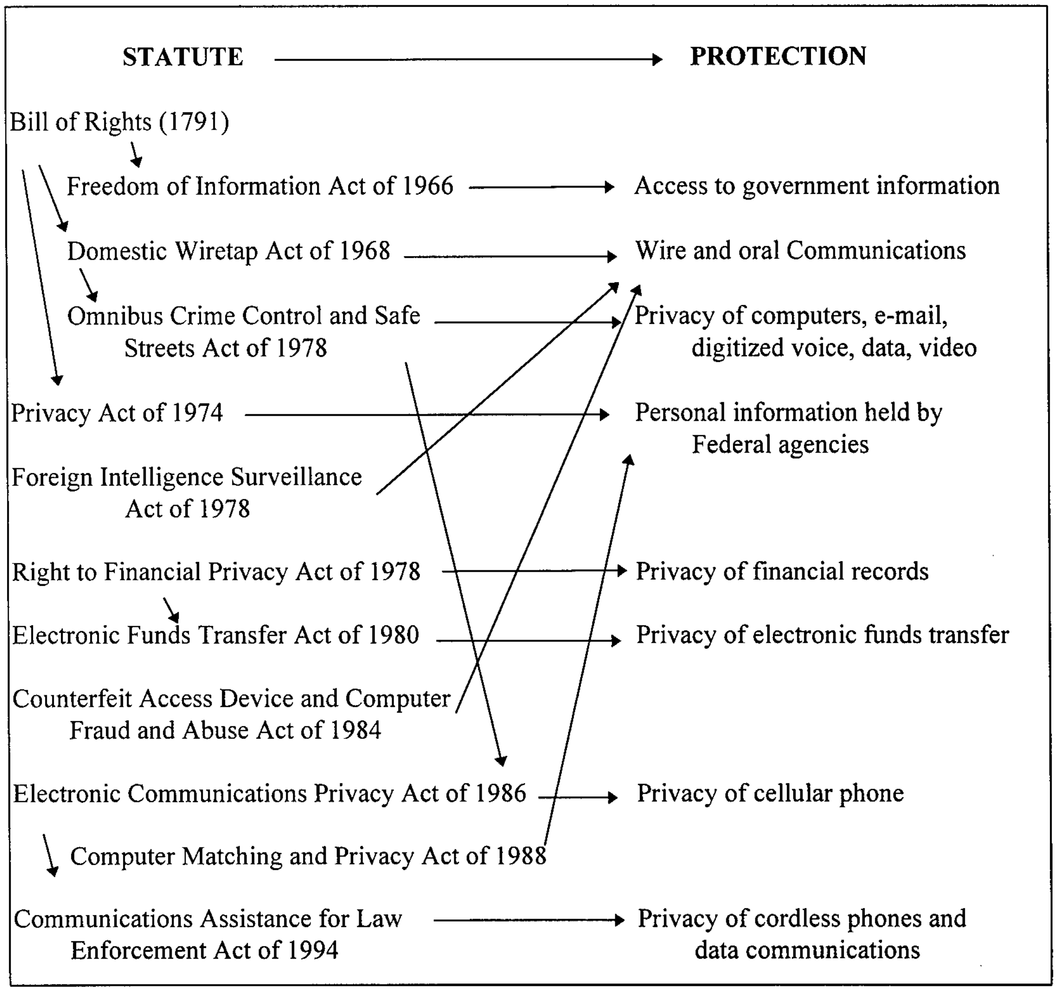
Several statutes address more than one of these objectives. For example, in an effort to guarantee individual *privacy*, Congress levied *security* requirements on Federal information systems containing personal information. The narrative will address the acts as they apply to the different objectives. These objectives and assigned roles and responsibilities of key statutes are summarized in Figures 2-2-9 through 2-2-15 at the end of this section. Other applicable statutes are summarized in the form of annotated bibliographies in Appendix A, References.

2.2.3.1 Protecting Individual Privacy and Providing Access to Government Information

Two aspects of individual privacy are subject to Federal legislation. The first is the protection of individuals' privacy from intrusion by third parties. Examples include protection against collection and dissemination of certain types of personal information (e.g., medical records, financial records, and arrest reports). The second aspect is the protection of individuals' privacy rights from intrusion by the government and governmental agencies (including law enforcement and intelligence agencies). This would include limitation on the government's ability to collect certain types of information (search and seizure and surveillance) and limitations on the ability of the government to disseminate information lawfully collected (e.g., tax information, privacy related information). A final goal of legislation—which is sometimes diametrically opposed to the goal of ensuring individual privacy—is ensuring citizens' access to information collected by the government.

The weight of privacy legislation makes it clear that Congress has taken its responsibility to guarantee a citizen's right to privacy seriously. Openness of the government—the availability of government information—to its citizens has also received Congressional attention. In 1966, the Freedom of Information Act required that government information, excluding national security, foreign relations, and certain law enforcement information, be made available to citizens. Concerned with the potential for abuse created by the massive amount of personal data held by government agencies, Congress passed the Privacy Act of 1974 and subsequent bills to limit the impact of technology on individual privacy and to state explicitly that, while general governmental information is assumed to be public information, information specific to any one individual is protected from disclosure.

As shown in Figure 2-2-2, Congress has chased technology for the last several years. The Privacy Act of 1974 arose from Congressional fear that automation was allowing federal agencies to accumulate an increasing amount of personal information. Focusing on information rather than the storage medium, the act requires the government to ensure reasonable safeguards as technology advances and as information becomes more easily accessible. Subsequent legislation, The Computer Matching and Privacy Act, restricted Federal use and disclosure of information resulting from computer matching capabilities. *Computer matching* compares information from different databases to detect fraud, waste, and abuse. As electronic fund transfers became commonplace, Congress required the financial community to ensure privacy equivalent to that provided when funds and financial information were transferred by mail or courier.



STATUTE → PROTECTION
Bill of Rights (1791)
Freedom of Information Act of 1966 → Access to government information
Domestic Wiretap Act of 1968 → Wire and oral Communications
Omnibus Crime Control and Safe Streets Act of 1978
Privacy of computers, e-mail, digitized voice, data, video
Privacy Act of 1974 → Personal information held by Federal agencies
Foreign Intelligence Surveillance Act of 1978
Right to Financial Privacy Act of 1978 → Privacy of financial records
Electronic Funds Transfer Act of 1980 → Privacy of electronic funds transfer
Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
Electronic Communications Privacy Act of 1986 → Privacy of cellular phone
Computer Matching and Privacy Act of 1988
Communications Assistance for Law Enforcement Act of 1994 → Privacy of cordless phones and data communications

Note: Arrows between the statutes indicate that subsequent statutes built upon or amended preceding statutes. Several statutes are indented from the left margin to make these relationships clearer. This indentation does not indicate a subordinate role or lesser effect.

Figure 2-2-2. Privacy and Access to Government Information

As technological capabilities advanced, Congress also found itself defining new methods of exchanging information in which a citizen had a legitimate expectation of privacy. Protection was initially extended to wire and oral communications in 1968 by the Domestic Wiretap Act. Subsequent amendments added computers, electronic mail (e-mail), and cellular phones to the list in 1986; cordless phones were added in 1994. Various types of data communications were defined and added by succeeding statutes. Today, unauthorized interception is illegal for almost every type of electronic or wire communication regardless of the type of information (e.g., voice, data, or video) or medium (e.g., cordless, cellular, or fiber optic) except for radio communications readily accessible to the general public. Any encrypted or scrambled information, even transmission techniques such as spread spectrum, are not considered readily accessible and therefore, unauthorized interception is illegal.

A note must be included on clandestine electronic intelligence gathering activities and the primacy of the privacy of U.S. citizens and residents. The Foreign Intelligence Surveillance Act of 1978 established a process to facilitate electronic acquisition of foreign intelligence within the United States while minimizing the impact on U.S. residents. Court orders are required unless the Attorney General, on behalf of the President, certifies in writing the purposes and procedures to be employed to minimize the impact on U.S. residents. Several other acts and Executive Orders assign intelligence gathering responsibilities, including oversight and jurisdiction. The Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) have purview over certain types of clandestine operations during peacetime. The FBI is responsible for foreign counter-intelligence operations (monitoring foreign agents and U.S. citizens for evidence of prohibited espionage activities) within the United States, while the CIA is the proponent for activities outside the United States. Foreign or domestic covert intelligence activities—which may include clandestine electronic intelligence gathering—require a Presidential intelligence finding (and in certain cases, notification of the appropriate Congressional committees) and must be coordinated with the CIA or the FBI. No agency except the CIA can conduct any special activities without a Presidential determination. As an exception, the Armed Forces may engage in special activities in time of war as declared by Congress or after the President has reported to Congress in accordance with the War Powers Resolution Act.

Figure 2-2-3 depicts a hierarchical chain of responsibility for ensuring individual privacy and citizen access to government information. The Department of Justice (DoJ) (including the Attorney General and the FBI) and the CIA are charged with minimizing the impact of intelligence and law enforcement activities on citizens. The Privacy Protection Study Commission has a charter encompassing federal, state, and local agencies. The Office of Management and Budget (OMB) publishes privacy guidelines and regulations for the Federal Government. OMB also has responsibility for government wide information technology management policy assigned by the Paperwork Reduction Act of 1980. These complementing responsibilities make OMB a significant player in the information assurance activities of the Federal Government.

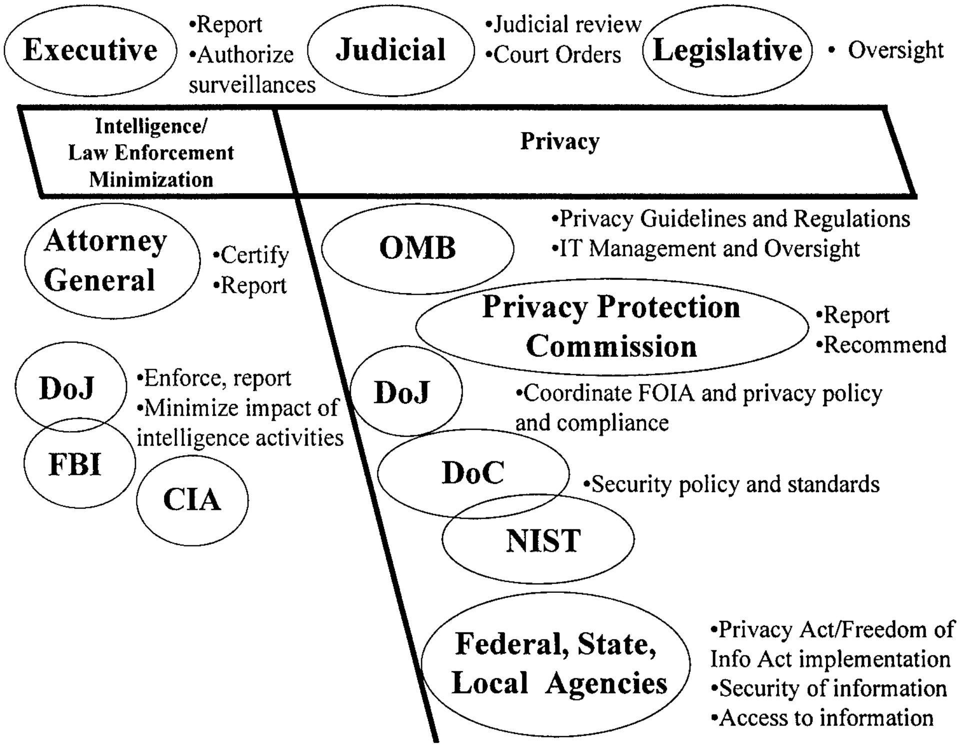

Executive
•Report
•Authorize surveillances
Judicial
•Judicial review
•Court Orders
Legislative
• Oversight
Intelligence/ Law Enforcement Minimization
Privacy
Attorney General
•Certify
•Report
DoJ
•Enforce, report
•Minimize impact of intelligence activities
FBI
CIA
OMB
•Privacy Guidelines and Regulations
•IT Management and Oversight
Privacy Protection Commission
•Report
•Recommend
DoJ
•Coordinate FOIA and privacy policy and compliance
DoC
•Security policy and standards
NIST
Federal, State, Local Agencies
•Privacy Act/Freedom of Info Act implementation
•Security of information
•Access to information

Figure 2-2-3. Government Responsibility for Ensuring Privacy

2.2.3.2 Securing Federal Information and Information Systems

This section focuses on those government organizations that have statutory responsibility for ensuring the security of Federal government information and information systems. Key to this discussion are categories of information. Statutes in support of this objective generally address information that is classified for reasons of national security or foreign policy, or information that is sensitive unclassified. Information or systems that are Warner Exempt are normally included with the classified information. These are systems that are exempt from the provisions of the Brooks Act of 1965 by the Warner Amendment because they involve command, control, communications, and intelligence (C3I), cryptography, or electronics embedded in weapons systems or equipment critical to a military or intelligence mission. However, policy documents often apply to the integrity and availability of all federal information and information systems, regardless of classification or sensitivity.

To assign security responsibilities, statutes have expanded roles assigned in preceding statutes. The Communications Act of 1934 gives OMB and the Department of Commerce (DoC) roles in executive branch telecommunications. The Federal Property and Administrative Services Act of 1949, the Brooks Act of 1965, and the Paperwork Reduction Act of 1980 give OMB, DoC, National Institute of Standards and Technology (NIST), and GSA roles in procuring and managing federal information technology. Because of these roles and efforts already under way in these agencies, the Computer Security Act of 1987 assigned responsibility for security standards and guidelines to DoC, NIST, NSA, and GSA for sensitive unclassified information. This act also established the Computer System Security and Privacy Advisory Board (CSSPAB). Executive Order 12356 subsequently established the Information Security Oversight Office (ISOO) under GSA to oversee compliance with national security information guidance. ISOO has been transferred to OMB.

Figure 2-2-4 portrays the applicable statutes, relationships, and assigned responsibilities. Parentheses indicate organizations with a regulatory role rather than statutory authority. Figure 2-2-5 provides a hierarchical view of assigned responsibilities for Federal INFOSEC.

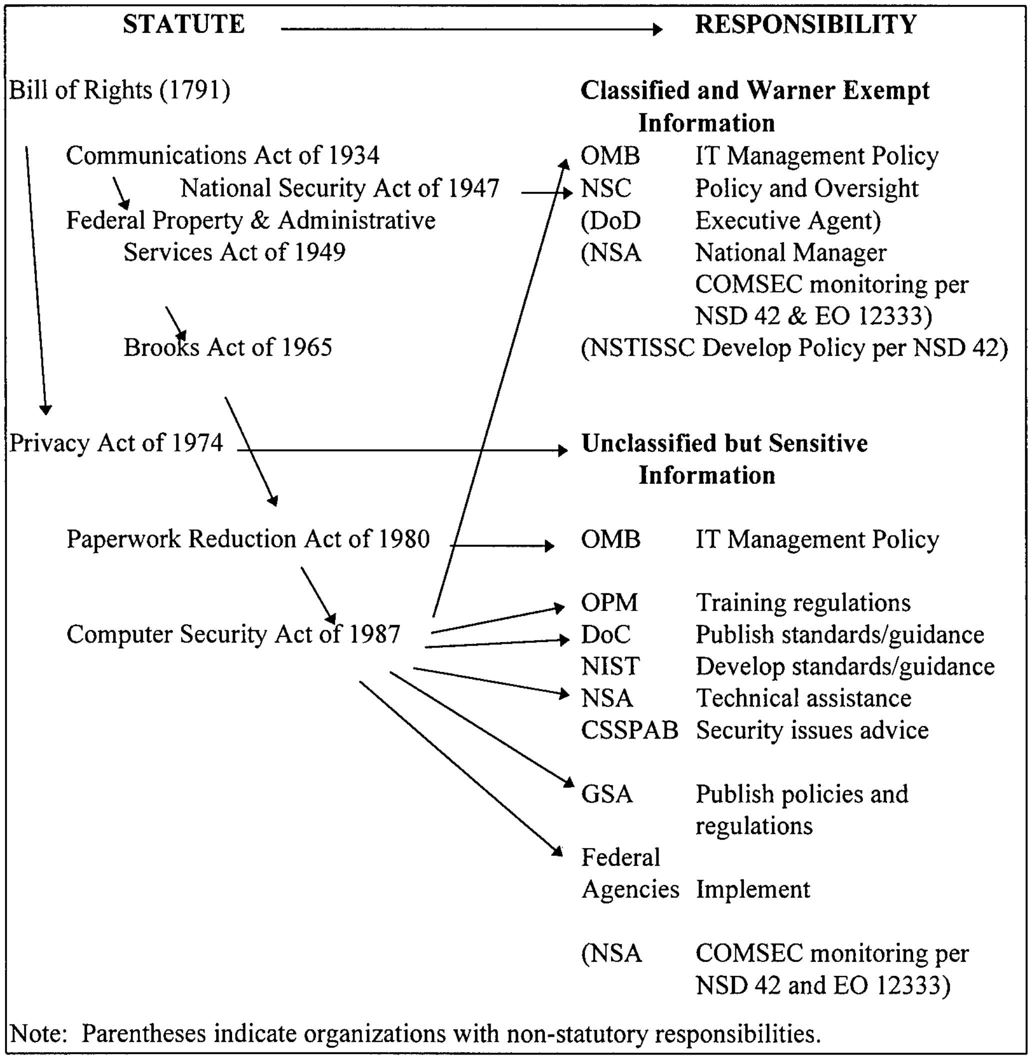
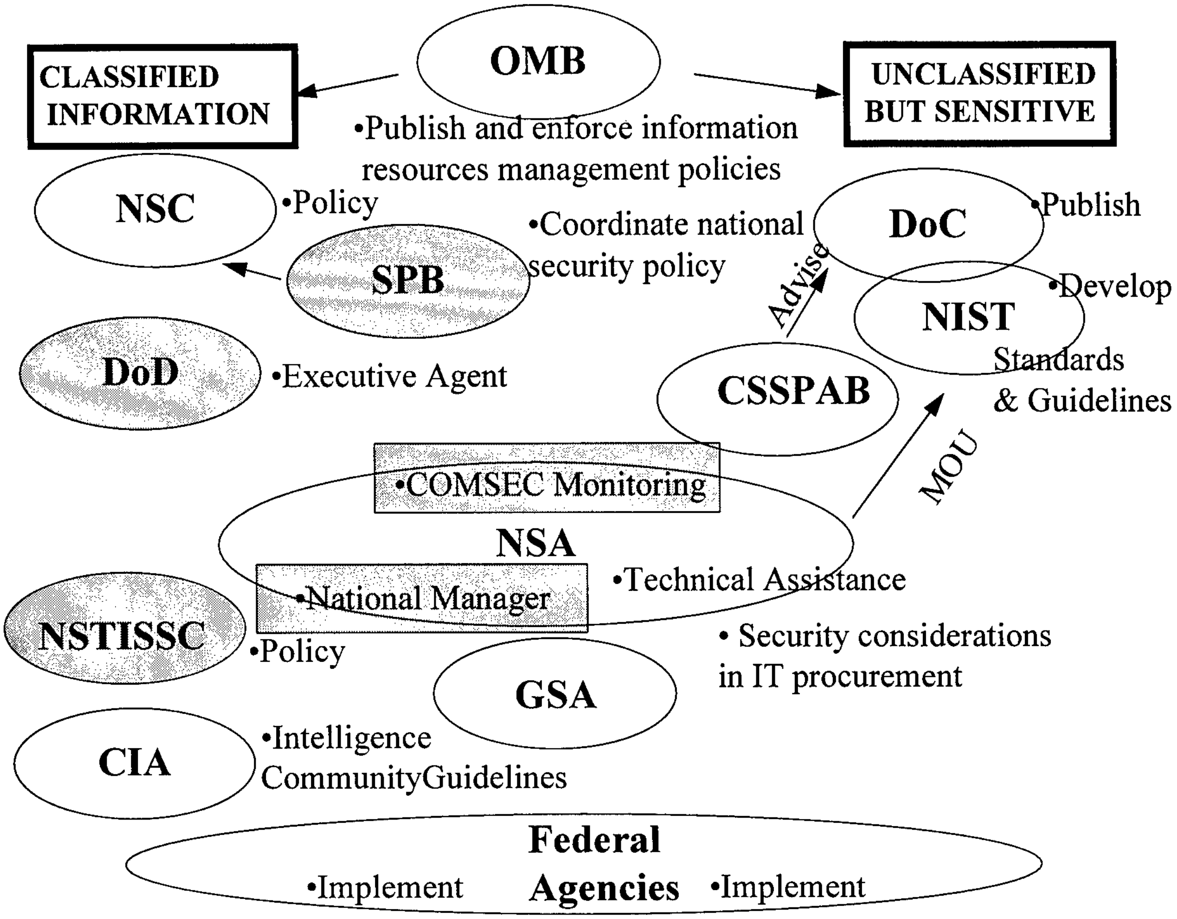

STATUTE
RESPONSIBILITY
Bill of Rights (1791)
Communications Act of 1934
National Security Act of 1947
Federal Property & Administrative Services Act of 1949
Brooks Act of 1965
Privacy Act of 1974
Paperwork Reduction Act of 1980
Computer Security Act of 1987
Classified and Warner Exempt Information
OMB IT Management Policy
NSC Policy and Oversight
(DoD Executive Agent)
(NSA National Manager COMSEC monitoring per NSD 42 & EO 12333)
(NSTISSC Develop Policy per NSD 42)
Unclassified but Sensitive Information
OMB IT Management Policy
OPM Training regulations
DoC Publish standards/guidance
NIST Develop standards/guidance
NSA Technical assistance
CSSPAB Security issues advice
GSA Publish policies and regulations
Federal Agencies Implement
(NSA COMSEC monitoring per NSD 42 and EO 12333)
Note: Parentheses indicate organizations with non-statutory responsibilities.

Figure 2-2-4. Security of Federal Information Systems


CLASSIFIED INFORMATION
OMB
UNCLASSIFIED BUT SENSITIVE
•Publish and enforce information resources management policies
NSC
•Policy
SPB
•Coordinate national security policy
DoC
•Publish
Advise
NIST
•Develop Standards & Guidelines
DoD
•Executive Agent
CSSPAB
MOU
•COMSEC Monitoring
NSA
•National Manager
•Technical Assistance
NSTISSC
•Policy
• Security considerations in IT procurement
GSA
CIA
•Intelligence CommunityGuidelines
Federal Agencies
•Implement
•Implement

Shading indicates organizations with non-statutory responsibilities.

Figure 2-2-5. Responsibility for Information Systems Security

It is important to provide a brief background of the Computer Security Act of 1987 to highlight sensitivities that remain today. In 1984, President Reagan signed National Security Decision Directive 145 (NSDD 145), National Policy On Telecommunications and Automated Information Systems Security. NSDD 145 appointed the Secretary of Defense the Executive Agent and the Director of NSA the National Manager for national telecommunications and information systems security. These roles made DoD responsible for sensitive unclassified information in addition to classified information. NSDD 145 encouraged the National Manager and Executive Agent to coordinate with the private sector on information systems security. Civil agencies and the private sector expressed concern that NSDD 145 gave the military and intelligence communities too much authority for non-national security information. Subsequent Administration actions, citing NSDD 145 as authority, heightened these concerns. The Computer Security Act of 1987 gave primary responsibility for sensitive unclassified standards and guidelines to the civil side of the Federal Government. President Bush signed National Security Directive 42 (NSD 42) in 1990 to bring Executive Branch policy in line with the act.

In 1989, NSA retained a key role for national security information, including sensitive unclassified. NSA and NIST executed a Memorandum of Understanding (MOU) in 1989 to clarify roles and responsibilities under the act. The MOU is not without controversy; some feel the MOU grants NSA greater responsibility for sensitive unclassified information than provided for in the act. Civil and private concern with centralizing policy development for classified and unclassified information under a single authority is still prevalent. An example of this concern can be seen in the organizational summary of the U.S. Security Policy Board, provided in Appendix A.

In summary, OMB has a prominent position within the Federal Government for all information technology policy and management, and significant roles in budget and privacy as well. OMB thus plays a key role in information assurance. The NSC plays a similar key role for national security information. Forums, in which both participate are key to future information and information system security policy. Policy makers interested in influencing the direction of information policy should monitor and participate in these forums.

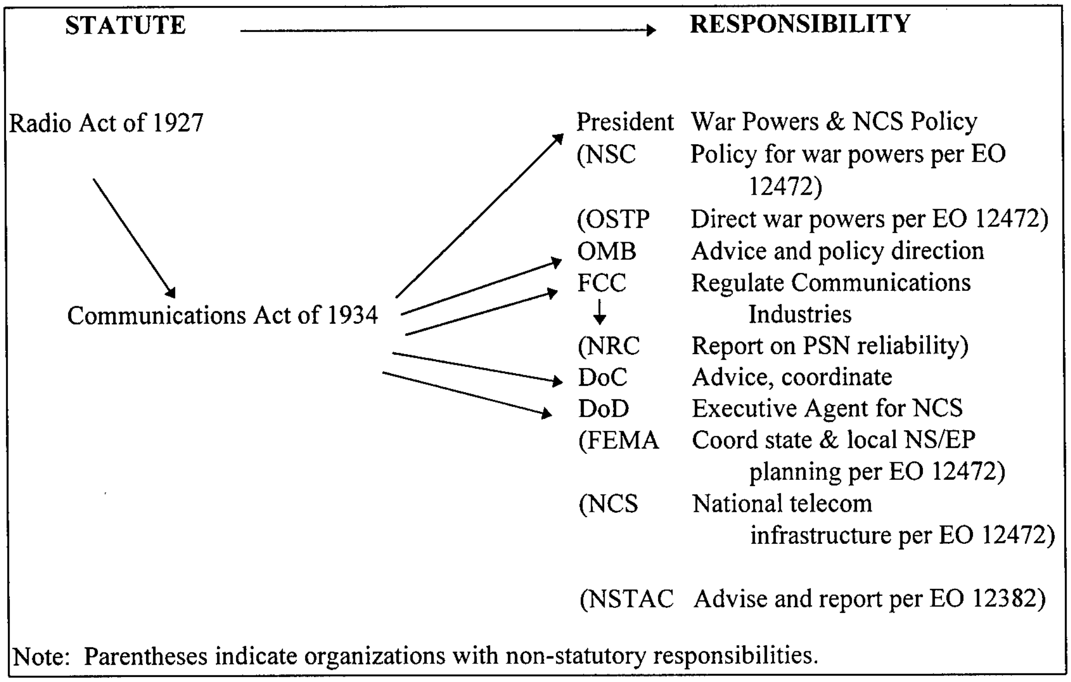
2.2.3.3 Ensuring Infrastructure Availability and Reliability

Early in the twentieth century, the Federal Government realized that reliability and availability of the telecommunications infrastructure was critical to national security and economic progress. In 1909, Congress passed a law, codified at Title 18, United States Code, Section 1362, which made it a crime to injure or destroy or interfere with any means of communication owned by the United States or used for military or civil defense functions of the United States. For the purposes of this discussion, however, “infrastructure” is not limited to government owned or leased telecommunications infrastructure, but includes the national public infrastructure as well.

The Communications Act of 1934 is the cornerstone to infrastructure reliability and availability. It created the Federal Communications Commission (FCC) to regulate the telecommunications and broadcast industries in the public interest and addressed willful or malicious interference with radio transmissions. The statute also delineated certain key war powers of the President in the area of telecommunications security, including the authority to require common carriers to give priority to national defense communications and employ the armed forces to prevent obstruction of interstate or foreign communications. Other Presidential and Executive Branch responsibilities under the Communications Act of 1934 are listed in Figure 2-2-9 on page 2-31.

Regulation of the telecommunications industry flows from Congress’ power to regulate interstate or foreign commerce. Regulation of the broadcast media—including television, radio and other public transmissions—flows from Congress’ power to regulate a scarce commodity—bandwidth, which may be allocated by the licensing procedures established by the FCC and Congress. The ability to regulate the scarce commodity allows legislative and executive control over the content of the broadcast media—a control which would otherwise be prohibited by the First Amendment’s guarantee of freedom of speech.

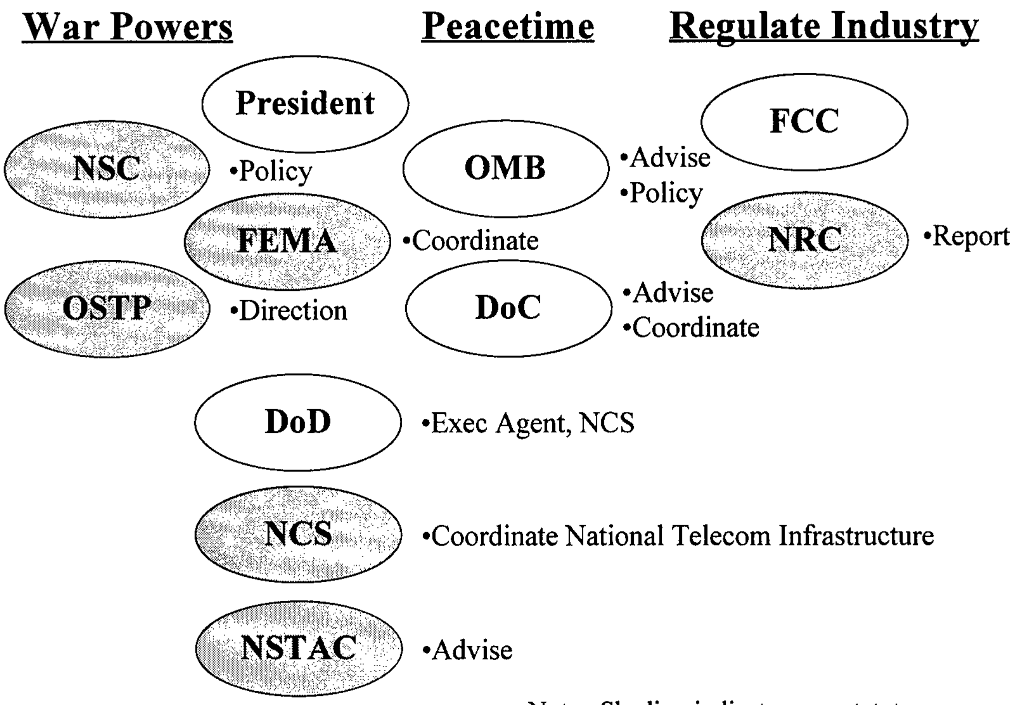
Figure 2-2-6 portrays the applicable statutes, relationships, and responsibilities of the infrastructure arising from the Radio Act and the Communications Act. Parentheses indicate organizations with a role in infrastructure availability and reliability that is not based upon statutory authority. Figure 2-2-7 portrays a hierarchical chain of responsibility for infrastructure availability and reliability. The President, FEMA, and others have roles during both war and peace. NSC, OSTP, OMB, and DoC are assigned responsibilities during either war or peacetime.



President	War Powers & NCS Policy
(NSC	Policy for war powers per EO 12472)
(OSTP	Direct war powers per EO 12472)
OMB	Advice and policy direction
FCC	Regulate Communications Industries
(NRC	Report on PSN reliability)
DoC	Advice, coordinate
DoD	Executive Agent for NCS
(FEMA	Coord state & local NS/EP planning per EO 12472)
(NCS	National telecom infrastructure per EO 12472)
(NSTAC	Advise and report per EO 12382)

Note: Parentheses indicate organizations with non-statutory responsibilities.

Figure 2-2-6. Infrastructure Availability and Reliability



Note: Shading indicates non-statutory responsibilities.

Figure 2-2-7. Responsibility for Infrastructure Availability and Reliability

Every Congress since the 73d Congress, which passed the Communications Act in 1934, has amended one or more sections of the act. Major overhauls of the act have generally not been successful. The 104th Congress will probably pass a major amendment, focusing on deregulation of the telecommunications industry. There are no indications that policy makers will use this opportunity to update Presidential war powers.

2.2.3.4 Defining the Criminality of Computer Fraud and Abuse

The same skills and techniques can be used in both computer crime and information warfare. While policy makers are currently debating the nature of an act of war in the Information Age, there is general agreement that computer crime must be better defined. To this end, the Clinton administration is preparing a High Technology Crime legislative proposal.

Computer crime has evolved along with technology and automation. So also have the legal views of computer crime. Initially, only crimes in which computers were used as tools were prosecuted. Embezzlement, for example, is a criminal act; therefore, embezzlement using computers was also a crime. However, trespassing into a computer, or examining computer generated files or data (without depriving the owner of these files or their use) was not considered a crime. Similarly, simply using a computer without the authorization of the owner was not considered a crime as long as the owner's use of the computer was not significantly affected. Finally, while paper documents could be stolen, the theft of computerized files and data presented difficult legal and proof problems.

As computer technology became more prevalent and better understood, views as to the criminality of computer fraud and abuse evolved. The Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the first Federal computer crime legislation. This statute was significantly overhauled in the Computer Fraud and Abuse Act (CFAA) of 1986. By this time, most of states had enacted legislation making theft of computer resources a criminal act. Even with statutes in place, however, computer crimes were often prosecuted as petty larceny, as the value of the stolen or damaged information did not translate easily into terms understood by judge or jury. It is now more commonplace for the value of the information to be considered and judgments rendered accordingly.

The CFAA amended Title 18, United States Code, Section 1030 to enhance penalties for intentional access into Federal Interest Computers for the purpose of committing certain types of criminal conduct. The CFAA term, *Federal Interest Computer*, defines the terms to include computers owned by or used by the Federal government in addition to a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State." Thus, *any* computer used in interstate or international commerce in the commission of the offense would also be covered by this provision. The statute criminalizes six computer activities: (1) the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or advantage a foreign nation; (2) the unauthorized access of a computer to obtain protected financial information; (3) the unauthorized access of a computer intended for the exclusive use of the Federal government; (4) the unauthorized interstate access of a computer system with an intent to defraud; (5) the unauthorized interstate or foreign access of computer systems that results in at least $1000 aggregate damage; and (6) the fraudulent trafficking in computer passwords affecting interstate commerce.

Each of these provisions requires proof that the defendant accessed the computer without authorization. By focusing on the method of *entry* into the computer or computer system, rather than the method of *use* of computer system, the statute excludes broad categories of potentially criminal conduct. Theft of information by corporate or government insiders, or those with an arguable right to access the computer, could not be punished under this provision. Nor could those who, with authorization to access or use a computer or computer system, alter, damage, or destroy information contained on that system. Similarly, the prosecution of authors or distributors of computer viruses or other forms of malicious code is complicated by the requirement that the government demonstrate the wrongdoer (1) actually accessed the computer; and (2) lacked the authority (explicit or implicit) to do so.

Curiously, the fraud provision of the CFAA expressly prohibits prosecution for the unauthorized access of a computer system where "the object of the fraud and the thing obtained consists only of the use of the computer." Thus, as under the wire fraud statute, the mere viewing of data without authorization may not be criminal under the CFAA. Furthermore, the protection afforded by the CFAA to national secrets, financial records, and government computers does not require an explicit computer crime statute; protection probably exists irrespective of the provisions of the CFAA. The anti-password provision of the CFAA is the most original section of the statute, but to date, there has not been a prosecution under this provision.

Perhaps the most famous application of this statute was the 1989 prosecution of Robert Tappan Morris, a Cornell University graduate student who, on November 2, 1988, released a computer worm across the Internet. The program, designed to surreptitiously spread across the network to thousands of connected computers, inadvertently replicated faster than the defendant intended, and, instead of inserting a copy or two into these networked computers, inserted thousands of copies of the program until the network actually shut down. On appeal, the second circuit rejected the defendant's arguments that, because he was permitted to send mail to users of computers on the network, he was therefore authorized to access these computers, and further rejected arguments the statute required proof he intended to cause damage to the computers—as distinct from intent to obtain unauthorized access.

Despite the successful prosecution in *Morris*, the predicted explosion of computer crime prosecutions has not occurred. The lack of prosecutions can be attributed to the fact that many computer crimes are committed by insiders to access the affected computers. In addition, corporations—especially institutions that depend upon public trust and confidence—are reluctant to report computer crimes which might tend to erode the public's faith. Moreover, there is a perception that computer offenders who cause no quantifiable loss to their victims, but nonetheless obtain confidential information about individuals or organizations, may evade effective punishment under the current Federal sentencing scheme.

Jurisdiction in computer crime is often cited as a problem as it transcends both state and national boundaries. In general, if an offense is wholly conducted within one state, the offense is a state crime. As Table 2-2-1 illustrates, virtually every state prohibits in some fashion the unauthorized access or use of computers. If the offense crosses state lines, or if the victim of the offense is the Federal Government, the offense is Federal. If the offense occurs internationally, it may constitute a crime in the country where the offender is located, where the victim is located, or in some instances, in the nation through which the communications travel. These definitions are not mutually exclusive, and an offense may violate local, state, Federal, national and international law simultaneously. Even if the conduct violates the statutes contained within a jurisdiction, a sovereign still must obtain personal jurisdiction over the defendant—that is, the sovereign must extradite the offender. In the United States, the Federal Government has nationwide jurisdiction, which may extend to the special maritime jurisdiction (U.S. territorial waters). However, to obtain jurisdiction abroad, the foreign country in possession of the accused must agree to turn the offender over to the United States—usually through extradition. Some countries do not prohibit unauthorized access of foreign systems. Most countries will not extradite unless the offense charged is a crime in that jurisdiction, and most nations are reluctant to extradite their own nationals.

Table 2-2-1. State Computer Crime Statutes

ALA. CODE §§ 13A-8-100 to 13A-8-103 (Supp. 1992)	MONT. CODE ANN. §§ 45-2-101, 45-6-310 to 45-6-311 (1991);
ALASKA STAT. § 11.46.740 (1989)	NEB. REV. STAT. §§ 28.1343 to 28.1348 (Supp. 1991);
ARIZ. REV. STAT. ANN. § 13-2316 (1989)	NEV. REV. STAT. ANN. §§ 205.473 to 205.491 (Michie 1992);
ARK. CODE ANN. §§ 5-41-101 to 5-41-107 (Michie Supp. 1991)	N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (1986);
CAL. PENAL CODE § 502 (West Supp. 1992)	N.J. STAT. ANN. §§ 2C:20-23 to 2C:20-34 (West Supp. 1992);
COLO. REV. STAT. §§ 18-5.5-101 to 18-5.5-102 (1986 & Supp. 1992)	N.M. STAT. ANN. §§ 30-45-1 to 30-45-7 (Michie Supp. 1989);
CONN. GEN. STAT. ANN. §§ 53a-250 to 53a-261 (West 1985)	N.Y. PENAL LAW §§ 156.00 to 156.50 (McKinney 1988);
DEL. CODE ANN. tit. 11, §§ 931 to 939 (1987 & Supp. 1993)	N.C. GEN. STAT. § 14-453 to 14-457 (1986);
FLA. STAT. ANN. §§ 815.01 to 815.07 (West Supp. 1993)	N.D. CENT. CODE ANN. § 12.1-06.1-08 (Supp. 1991);
GA. CODE ANN. §§ 16-9-91 to 16-9-94 (1992)	OHIO REV. CODE ANN. §§ 2913.01, 2913.81 (Anderson 1993);
HAW. REV. STAT. §§ 708-890 to 708-893 (Supp. 1992)	OKLA. STAT. ANN. tit. 21, §§ 1951 to 1958 (West Supp. 1993);
IDAHO CODE §§ 18-2201 to 18-2202 (1987)	OR. REV. STAT. §§ 164.125, 164.377 (1991); 18
ILL. ANN. STAT. Ch. 38 para. 16D-1 to 16D-7 (Smith-Hurd Supp. 1992)	PA. CONS. STAT. ANN. § 3933 (Supp. 1992);
IND. CODE ANN. §§ 35-43-1-4 & 35-43-2-3 (Burns Supp. 1992)	R.I. GEN. LAWS §§ 11-52-1 to 11-52-8 (Supp. 1992);
IOWA CODE ANN. §§ 716A.1 to 716A.16 (West Supp. 1992)	S.C. CODE ANN. §§ 16-16-10 to 16-16-30 (Law. Co-op. 1985);
KAN. STAT. ANN. § 21-3755 (1988)	S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 43-43B-8 (1983 & Supp. 1992);
KY. REV. STAT. ANN. §§ 434.840 to 434.860 (Michie/Bobbs-Merrill 1985)	TENN. CODE ANN. §§ 39-14-601 to 39-14-603 (1991);
LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (West 1986 & Supp. 1993)	TEX. PENAL CODE ANN. §§ 33.01 to 33.05 (West 1989 & Supp. 1992);
ME. REV. STAT. ANN. tit. 17-A, § 357 (West 1983 & Supp. 1992)	UTAH CODE ANN. §§ 76-6-701 to 76-6-705 (1990);
MD. ANN. CODE art. 27, § 146 (Supp. 1991)	VA. CODE ANN. §§ 18.2-152.1 to 18.2-152.14 (Michie 1988 & Supp. 1992);
MASS. GEN. L. Ch. 266, § 30 (1990)	WASH. REV. CODE §§ 9A.52.110 to 9A.52.130 (1988);
MICH. STAT. ANN. § 28.529 (Callaghan 1990)	W. VA. CODE §§ 61-3C-1 to 61-3C-21 (Supp. 1992);
MINN. STAT. ANN. §§ 609.87 to 609.891 (West 1987 & Supp. 1992);	WIS. STAT. § 943.70 (Supp. 1992);
MISS. CODE ANN. §§ 97-45-1 to 97-45-13 (Supp. 1992)	WYO. STAT. §§ 6-3-501 to 6-3-505 (1988)
MO. REV. STAT. §§ 537.525, 569.093 to 569.099 (1986 & Supp. 1991);	States not listed had no computer crime statutes as of January 1995.

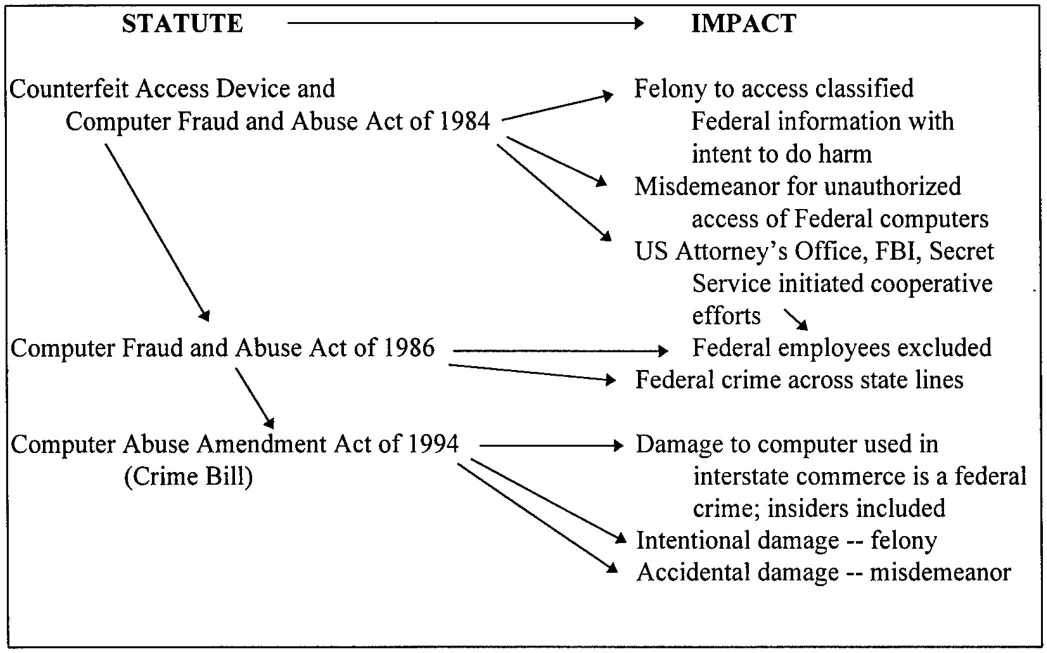
Table 2-2-2 shows examples of jurisdiction. This table oversimplifies a very complex process involving Federal and State law, the laws of foreign countries, and international agreements.

Table 2-2-2. Computer Crime Jurisdiction

ACT	JURISDICTION
Intruder and system in one state	State
Intruder in one state; system in another	Federal
Intruder penetrates a system used in interstate commerce or communications	Federal
Intruder penetrates a Federal system in the U.S.; intent criminal	FBI; United States Secret Service
Intruder penetrates a Federal system in the U.S.; intent espionage	FBI; National Security
Foreign citizen hacks a U.S. system which displays a warning banner; no foreign law in place	Apprehension and adjudication can be pursued through existing treaties
Foreign citizen hacks a U.S. system which displays a warning banner; Foreign law in place.	U.S. or Foreign law; by agreement.

Jurisdiction is not the real problem. Processes, though cumbersome, are in place both nationally and internationally to resolve issues. The real problem is determining intent and coordinating jurisdiction in real-time. Policy makers may consider putting detection vehicles in place and providing for consolidated and coordinated apprehension of computer criminals. Early detection and apprehension will reduce potential damage and may serve as a useful deterrent. It may be more effective to table issues of intent until after apprehension. The FBI has taken steps in this direction by establishing a Computer Crime Team, made up of representatives from both the Criminal and National Security Divisions in California.

Figure 2-2-8 portrays the relevant statutes and impacts of the criminality of computer fraud and abuse. Acts associated with intellectual property rights, copyright law, and the banking and financial industries are not shown, as they are generally outside the purview of DoD. However, DoD policy makers should keep in mind that government-wide technical solutions and policy must encompass these issues because they are important to the civil agencies of the Federal Government and to the private sector.



STATUTE → IMPACT

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

- Felony to access classified Federal information with intent to do harm
- Misdemeanor for unauthorized access of Federal computers
- US Attorney's Office, FBI, Secret Service initiated cooperative efforts

Computer Fraud and Abuse Act of 1986

- Federal employees excluded
- Federal crime across state lines

Computer Abuse Amendment Act of 1994 (Crime Bill)

- Damage to computer used in interstate commerce is a federal crime; insiders included
- Intentional damage -- felony
- Accidental damage -- misdemeanor

Figure 2-2-8. Criminality of Computer Fraud and Abuse

2.2.4 International Legal Environment

Law among nations is not codified in a body of international law. The International Court of Justice recognizes customary international law; that is, law which is common to many nations, as well as international treaties or conventions, such as the Geneva Conventions. Few countries have laws which adequately address computer crime. Among those countries with computer crime statutes, there is no general agreement on the type of conduct that constitutes computer crime. Nor are there any international treaties or conventions which address computer fraud and abuse. Investigation, apprehension and adjudication of computer criminals, must rely on domestic law and mutual assistance agreements in the form of bilateral and multilateral treaties and agreements. Generally, these agreements require *mutual criminality*; that is, an offense must be a crime in both countries for the foreign country to take legal action. Prosecution of international computer criminals can be an unwieldy process complicated by domestic privacy, search and seizure laws, and jurisdictional considerations. Recognizing the problem, and recognizing that international trade is enhanced by trusted electronic communications, the international community has initiated efforts to *harmonize* international law. Both the Organization for Economic Cooperation and Development (OECD) and the Council of Europe have proposed activities that should be criminalized by member nations. The OECD also issued guidelines for the security of information systems. The IITF Security Issues Forum recently recommended the United States adopt these guidelines.

The United States must also consider the potential effect of its IW activities on other sovereign nations. Some agreements, such as the INTELSAT agreement, may bound U. S. IW activities, while others such as the North Atlantic Treaty or other regional mutual defense agreements may facilitate activities. International organizations in which the United States maintains membership, such as the International Criminal Police Organization (INTERPOL) may also help law enforcement authorities.

In general, it is difficult to determine how various agreements and organizations may effect information warfare activities. A knowledgeable General Counsel can, however, determine the international implications of specific policies or planned operations. Therefore, to ensure that offensive and defensive information warfare activities operate within the bounds and authorities of the international legal environment, knowledgeable General Counsel should be involved in IW policy formulation, planning, and operations.

Figures 2-2-9 through 2-2-15 summarize key statutes relevant to the four objectives discussed in this section.

COMMUNICATIONS ACT OF 1934

Purpose, General Provisions, Assigned Responsibilities, and Functions

Purpose: The purpose of the Communications Act of 1934 is to regulate interstate and foreign communications by wire and radio in the public interest. The act establishes the Federal Communications Commission, assigns war powers to the President, addresses radio stations operated by foreign governments, and willful or malicious interference with radio transmissions.

NOTE: Every Congress, since the 73d Congress passed the original act in 1934, has amended one or more sections of the act while in session; however, attempts at major overhauls of the act have not passed.

General Provisions:

- Established the Federal Communications Commission
- Unauthorized interception and disclosure of communications by wire or radio prohibited.

Assigned Responsibilities and Functions

President:

- War powers:
  - During any war in which the U. S. is engaged, the President may:
    - Order any carrier to give preference or priority for national defense communications
    - Employ armed forces to prevent retarding or obstruction of interstate or foreign communications.
  - Upon proclamation that war or threat of war exists, the President may:
    - Amend or suspend rules and regulations pertaining to any stations capable of emitting electromagnetic radiations.
    - Close and remove any emitting device that may serve as a navigational device.
    - Amend rules pertaining to wire communications
    - Order the closure or government use of wire facilities
- Policy direction of the development and operation of a National Communications System
- Coordinating policy, plans, and programs for the mobilization and use of the Nation's telecommunications resources in an emergency.

Office of Management and Budget:

- Serve as President's principal adviser on procurement and management of Federal telecommunications systems
- Developing policies for the procurement and management of Federal telecommunications systems
- Final disposition of appeals on frequency assignments made by Secretary of Commerce.

Secretary of Commerce:

- Serve as **President's principal adviser on telecommunications policies** pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry.
- **Advise the Director of the Office of Management and Budget on** the development of **policies relating to the procurement and management of Federal telecommunications systems.**
- **Conduct studies and evaluations concerning** telecommunications research and development and concerning the initiation, improvement, expansion, testing, operation, and use of **Federal telecommunications systems**. Study and report on the impact of the convergence of computers and communications technology. Advise OMB and others of the results of these studies.

Figure 2-2-9. Communications Act of 1934

Secretary of Commerce (Continued)

- **Develop** and set forth in coordination with the Secretary of State and other interested agencies plans, **policies, and programs which relate to international telecommunications issues**.
- **Coordinate telecommunications activities of the Executive Branch**, including interoperability, privacy, security, spectrum use, and emergency readiness.
- **Establish interagency groups and advisory committees** as required.
- Manage electromagnetic spectrum
- Evaluate and recommend remedial actions for the capabilities of telecommunications resources
- Instruct Communications Satellite Organization in its role as representative to INTELSAT.

Secretary of State:

- In the conduct of foreign policy, coordinate with and consider Federal Communications Commission's regulatory and policy responsibilities.
- Direct foreign relations with regard to the Communications Satellite Act of 1962.

Federal Communications Commission:

- Regulate interstate and foreign commerce in communication by wire and radio as required by this act, as amended.
- Report annually to Congress information and data that may be considered of value and any specific recommendations as to additional legislation considered necessary or desirable including all legislative proposals submitted to OMB.

Figure 2-2-9. Communications Act of 1934 (Continued)

PRIVACY ACT OF 1974

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: The objective of the Privacy Act of 1974 is to protect personal privacy from invasions by Federal agencies, in light of increasing use of information technology in the Federal government and the associated increase in personal information maintained by Federal agencies. The law allows individuals to specify what information may be held by a government agency and gives individuals the right to obtain information held on them by the Federal government.

General Provisions:

- The Act levied civil and criminal penalties for violations of the provisions of the Act.
- The Act requires physical security practices, information management practices, and computer and network controls necessary to ensure individual privacy.

Assigned Responsibilities and Functions:

President:
- Submit an annual report to the Speaker of the House and President pro tempore of the Senate.

Privacy Protection Study Commission:
- Study automation practices and privacy issues at federal, state, and local level.
- Recommend legislation, regulation, policy to protect individual privacy.

Office of Management and Budget:
- Develop guidelines and regulations.

Federal Agencies:
- Not disclose personal information without written consent or under specified conditions.
- Account for disclosures.
- Upon request, allow individuals access to information maintained on them.
- Minimize records maintained to those required for business.
- Identify how information will be used on forms requesting information.
- Publish in the Federal Record new or revised systems containing personal information.
- Publish rules implementing provisions of the Act.
- Not sell or rent an individual's name and address.
- Notify OMB and Congress in advance of any proposal to establish or alter any system of records.

Figure 2-2-10. Privacy Act of 1974

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: The President may authorize electronic surveillance without a court order to acquire foreign intelligence information in the United States. Other Federal officers, with the approval of the Attorney General, may request court orders for approval to conduct electronic surveillance. Probable cause of criminal activity is not required. Special seven member court is established to authorize surveillances. The Act prescribes the time limits and procedures that must be followed with or without a court order. Terms are defined including minimization procedures which are procedures that must be taken to prohibit the dissemination and minimize the acquisition and retention of nonpublic information gathered on non-consenting United States persons.

General Provisions:

- Targets of electronic surveillance will be agents of foreign powers as defined in the Act.
- Minimization techniques will be used to reduce acquisition of information on United States persons.
- Information acquired concerning a United States person may not be disclosed without consent except in accordance with prescribed procedures.
- Court orders are required; the President, if the situation warrants, may authorize electronic surveillance in accordance with prescribed procedures.
- Grants President limited--fifteen days--exclusion during time of declared war.
- Assigns criminal and civil liability

NOTE: Some forms of foreign electronic intrusion might be considered outside of the scope of this act. A foreign power, as defined in Section 1801, must be linked to a foreign government or political organization. International terrorism is an exception to this political or national affiliation but is defined as involving violent acts or acts dangerous to human life. If the Drug Cartels are considered foreign powers under the terms of this Act, then most organized or sponsored electronic intrusions should be as well.

Assigned Responsibilities and Functions

President:

- Authorize, through the Attorney General, electronic surveillance to acquire foreign intelligence information without a court order.

Attorney General:

- Certify in writing, under oath, that the foreign intelligence information to be gathered will likely not acquire communications by United States persons, and that proposed minimization procedures are in accordance with the law.
- Transmit a copy of the certification to the court established by this act
- Report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.
- Assess compliance with published minimize procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.
- May direct a specified common carrier aid electronic surveillance efforts. The carrier will be compensated for the aid provided.
- Submit annual reports to Congress regarding the number of applications, orders and extensions.
- Report semiannually on all electronic surveillance under the Act.

Figure 2-2-11. Foreign Intelligence Surveillance Act of 1978

Director of Central Intelligence:

- Provide consultation to the Chief Justice on appropriate security measures for safeguarding the Attorney General certifications under his act.
- Provide consultation to the common carriers on appropriate security measures for safeguarding electronic surveillance operations.

Court Established by this Act:

- Issue court orders based upon requests having met the requirements of this act.
- Maintain requests under security measures established by the Chief Justice with the concurrence of the Attorney General.

Other Federal Officers:

- May make applications for court orders based upon the approval of the Attorney General and certification by a senior Executive Branch official responsible for national security or defense.

Communication Common Carriers:

- Furnish information, facilities, or technical assistance as necessary and as directed by the Attorney General. Carriers will be compensated for support rendered.
- Maintain secrecy of the operation and records.

Figure 2-2-11. Foreign Intelligence Surveillance Act of 1978 (Continued)

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: To update Federal privacy provisions; incorporating new technology and capabilities.

General Provisions:

- The definition of electronic communication system includes and wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities for the electronic storage of communications.
- "Communications Common Carriers" is changed to "providers of wire or electronic communication" services.
- Remains legal to intercept electronic communications that are readily accessible to the general public unless such interception causes interference to lawful receivers.
- Authorizes civil damages for the any person whose wire, oral, or electronic communications is illegally intercepted, disclosed, or used.
- The act does not prohibit the interception of encrypted or other executive branch official communications by authorized officers of the government for communications security or for under the Foreign Intelligence Surveillance Act of 1978.
- Penalties are levied against those divulging the plan or existence of a legal surveillance.
- The Attorney General may request an injunction against anyone who is engaged or plans to engage in a felony violation of this act.
- Unlawful access or divulgence of electronically stored communications or electronic communicate service or remote computing service is illegal.
- Government entities may request a court order to require service providers to make a backup copy of records or communications.
- Court orders are required for pen registers or trap and trace devices except for normal carrier operations and maintenance or with user authorization.
- Intentional or malicious interference with the operation of a communications or weather satellite is illegal.

Assigned Responsibilities and Functions:

<u>Attorney General</u>:

- Annually report to Congress on the number of pen register/trap and trace orders requested by law enforcement agencies of the Department of Justice.

<u>Federal Bureau of Investigation</u>:

- May request subscriber information, toll billing and transactional records with written certification that the information is relevant to a foreign counterintelligence investigation or that the individual is an agent of a foreign power as defined in the Foreign Intelligence Surveillance Act of 1978.
- The FBI may disseminate obtained information to other government agencies with relevant responsibilities.
- The Director of the FBI will report to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually on these requests.

Figure 2-2-12. Electronic Communications Privacy Act of 1986

COMPUTER SECURITY ACT OF 1987

Purpose, Assigned Responsibilities and Functions

Purpose: To improve the security and privacy of sensitive information in Federal computer systems by establishing minimum acceptable security practices. The act emphasizes risk-based, cost-effective security and establishes the Computer System Security and Privacy Advisory Board within the Department of Commerce.

Assigned Responsibilities and Functions

President:

- Disapprove or modify standards and guidelines published by the Secretary of Commerce pertaining to Federal computer systems. This authority may not be delegated.

Office of Personnel Management:

- Issue regulations prescribing procedures and scope for training of Federal civilian employees.

Secretary of Commerce:

- Promulgate compulsory and binding standards and guidelines pertaining to Federal computer systems.
- Waive, in writing, compulsory or binding standards if it can be proven that compliance would adversely effect mission accomplishment of a Federal computer system.
- Notice of waiver must be transmitted to Committee on Government operations of the House of Representatives and the Committee on governmental Affairs of the Senate
- Limitations: Authority is subject to direction by the President and Office of Management and Budget.

National Institute of Standards and Technology:

- Responsible for developing standards and guidelines for Federal computer systems including cost-effective security and privacy of sensitive information.
- NIST should draw upon the technical advice and assistance, including work products, of the National Security Agency.
- Submit standards and policies to the Secretary of Commerce for promulgation along with recommendations as to the extent they should be made compulsory or binding.
- Develop guidelines for training employees in security awareness and practices.
- Assist the private sector, upon request.
- Make recommendations to GSA on policies and regulations.
- Provide technical assistance to operators in implementing standards and guidelines.
- Ensure, to the maximum extent possible, that standards for sensitive information are consistent and compatible with standards for classified information.

General Services Administration:

- Revise Federal information resource management regulations to be consistent with standards and guidelines promulgated by the Secretary of Commerce.
- Limitations: Authority is subject to direction by the President and Office of Management and Budget.

Figure 2-2-13. Computer Security Act of 1987

Federal Agencies:

- May promulgate standards for cost-effective security and privacy of sensitive information that are more stringent than standards promulgated by the Secretary of Commerce, as long as, compulsory and binding provisions are included.
- Provide mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems containing sensitive information.
- Identify each Federal computer system which contains sensitive information.
- Establish security plans for each system identified above and provide copies to NIST and NSA.

Federal Computer System Operators:

- Establish security plans for all computer systems that contain sensitive information.

Computer System Security and Privacy Advisory Board:

- Identify emerging issues relative to computer systems security and privacy.
- Advise NIST and Secretary of Commerce on security and privacy issues pertaining to Federal computer systems.
- Report findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and appropriate committees of Congress.

Figure 2-2-13. Computer Security Act of 1987 (Continued)

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: To make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes.

General Provisions:

- Law enforcement agency cannot require any specific design of equipment or facilities.
- Requirements do not apply to information service providers or private networks and interconnection services and facilities.
- Carriers are not responsible for decrypting communication unless the encryption is provided by the carrier and the carrier is capable of decrypting.
- Cordless telephones and modulation techniques "the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication." are included under the "expectation of privacy" clause. Unauthorized interception is illegal.

Assigned Responsibilities and Functions:

Attorney General:

- Establish capacity requirements for the number of simultaneous interceptions, pen registers, and trap and trace devices.
- Reimburse carriers for costs directly associated with modifications necessary to comply with the act.

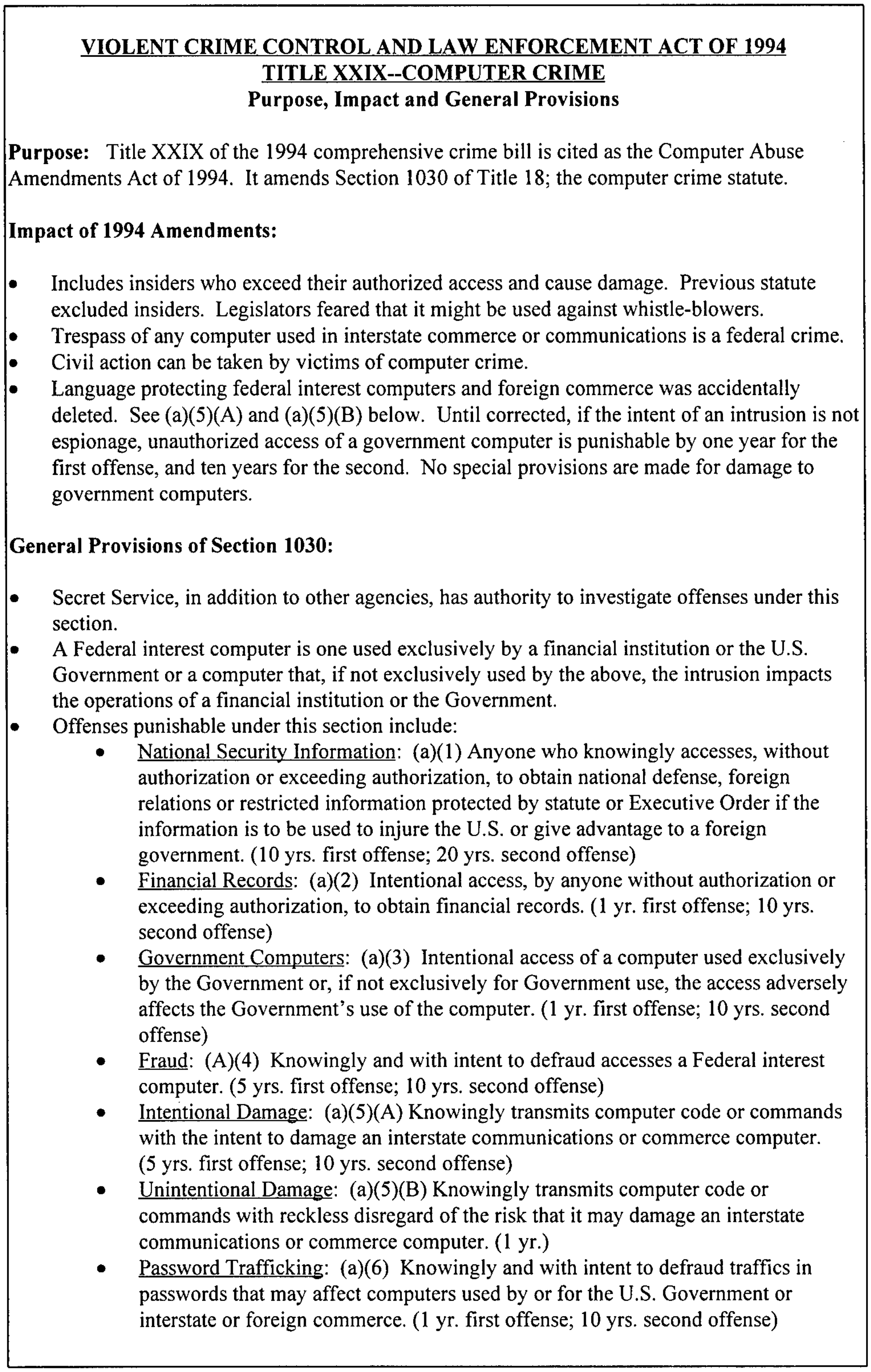
Federal Communications Commission:

- Prescribe rules necessary to implement the act.

Telecommunications Carriers:

- Shall ensure that its equipment or facilities that provide customer services are capable of isolating and interception and providing call-identification of all wire and electronic communications.
- Ensure activation of this capability is restricted to court order or other lawful authorization.

Figure 2-2-14. Communications Assistance for Law Enforcement Act of 1994



VIOLENT CRIME CONTROL AND LAW ENFORCEMENT ACT OF 1994
TITLE XXIX--COMPUTER CRIME
Purpose, Impact and General Provisions

Purpose: Title XXIX of the 1994 comprehensive crime bill is cited as the Computer Abuse Amendments Act of 1994. It amends Section 1030 of Title 18; the computer crime statute.

Impact of 1994 Amendments:

- Includes insiders who exceed their authorized access and cause damage. Previous statute excluded insiders. Legislators feared that it might be used against whistle-blowers.
- Trespass of any computer used in interstate commerce or communications is a federal crime.
- Civil action can be taken by victims of computer crime.
- Language protecting federal interest computers and foreign commerce was accidentally deleted. See (a)(5)(A) and (a)(5)(B) below. Until corrected, if the intent of an intrusion is not espionage, unauthorized access of a government computer is punishable by one year for the first offense, and ten years for the second. No special provisions are made for damage to government computers.

General Provisions of Section 1030:

- Secret Service, in addition to other agencies, has authority to investigate offenses under this section.
- A Federal interest computer is one used exclusively by a financial institution or the U.S. Government or a computer that, if not exclusively used by the above, the intrusion impacts the operations of a financial institution or the Government.
- Offenses punishable under this section include:
  - National Security Information: (a)(1) Anyone who knowingly accesses, without authorization or exceeding authorization, to obtain national defense, foreign relations or restricted information protected by statute or Executive Order if the information is to be used to injure the U.S. or give advantage to a foreign government. (10 yrs. first offense; 20 yrs. second offense)
  - Financial Records: (a)(2) Intentional access, by anyone without authorization or exceeding authorization, to obtain financial records. (1 yr. first offense; 10 yrs. second offense)
  - Government Computers: (a)(3) Intentional access of a computer used exclusively by the Government or, if not exclusively for Government use, the access adversely affects the Government's use of the computer. (1 yr. first offense; 10 yrs. second offense)
  - Fraud: (A)(4) Knowingly and with intent to defraud accesses a Federal interest computer. (5 yrs. first offense; 10 yrs. second offense)
  - Intentional Damage: (a)(5)(A) Knowingly transmits computer code or commands with the intent to damage an interstate communications or commerce computer. (5 yrs. first offense; 10 yrs. second offense)
  - Unintentional Damage: (a)(5)(B) Knowingly transmits computer code or commands with reckless disregard of the risk that it may damage an interstate communications or commerce computer. (1 yr.)
  - Password Trafficking: (a)(6) Knowingly and with intent to defraud traffics in passwords that may affect computers used by or for the U.S. Government or interstate or foreign commerce. (1 yr. first offense; 10 yrs. second offense)

Figure 2-2-15. Violent Crime Control and Law Enforcement Act of 1994

2.3 REGULATORY ENVIRONMENT

2.3.1 Introduction

The Federal Government regulates industry and Federal information warfare activities in three ways:

- By passing laws and issuing orders and regulations.
- Through the activities of regulatory agencies.
- Through export control.

2.3.2 Orders and Regulations

This section will address orders and regulations. Executive Orders are formal policy documents issued by the President of the United States. Normally, Executive Orders either precede or implement law. They are published in the U.S. Code of Federal Regulations and, unless classified, are frequently reprinted with relevant statutes in the U.S. Code Annotated. Other documents such as Presidential Proclamations, Memoranda, and Directives are equally formal but have more specialized functions. Orders and regulations are issued to achieve some of the same basic goals of legislation:

- To ensure the availability of telecommunications infrastructure, particularly for national defense purposes.
- To regulate the communications facilities in the public interest.
- To provide access to governmental documents.
- To protect certain classes of information from unauthorized disclosure (for example, classified information).
- To preserve individual privacy.
- To define the limits of authorized and unauthorized behavior.
- To define administrative responsibility.

Executive Order 12333 is significant because it makes the Secretary of Defense the Executive Agent for signals intelligence and COMSEC for the Federal Government. NSA executes this responsibility on behalf of the Secretary of Defense. Executive Order 12356 gives overall policy direction responsibility for national security information to the NSC and establishes the ISOO under the GSA to develop directives to implement the order and oversee compliance. Executive Order 12472 assigns responsibilities for telecommunications to support national security/emergency preparedness (NS/EP). These assignments complement statutory responsibilities for Federal information security, infrastructure reliability, and availability. Figures 2-2-5 and 2-2-7, on pages 2-21 and 2-24, depict these assignments of non-statutory responsibilities.

Executive Order 12382 establishes the NSTAC. Appendix A includes a summary of the NSTAC organization and roles. In addition to its role as a presidential advisory committee, meetings between the NSTAC and the NCS Committee of Principals (COP) serve as useful forums for exchange of information between industry and government. An outgrowth of the NSTAC, the Network Security Information Exchange (NSIE) serves as a valuable forum for information exchange between industry representatives.

The U.S. Code of Federal Regulations (CFR) is a codification of the general and permanent rules published in the Federal Register (FR) by the Executive departments and agencies of the Federal government. The CFR describes the legislative basis, goals, and predominant policies of the Federal Government. In effect, it implements law and Executive Orders. Agency instructions are published as well as Action sections identifying requirements for Federal agencies. Unless otherwise noted, Federal regulations published in the CFR after notice and comment are binding on both the government agencies and those regulated by these agencies. Though many titles and chapters are relevant to information warfare, only two exemplary sections are noted in Appendix B, References: Federal Information Management Regulation (41 CFR 201) and Chapter II, Title 47 describing NS/EP responsibilities.

It is unlikely that policy makers will target the CFR to make significant changes in Federal operations. The CFR does, over time, reflect legal and regulatory changes in the form of implementing regulations. As a reference, the CFR is useful as it is a readable and comprehensive compilation of existing macro- and micro-Federal guidance.

As a final note, the Uniform Commercial Code (UCC) is applicable to both civil agencies and the private sector. The UCC standardizes the laws in States relating to sales and secured transactions. Sponsored by the National Conference of Commissioners on Uniform State Laws and the American Law Institute, the UCC has been adopted by virtually all states (some with amendment) but has not been adopted by the Federal Government. Federal commercial law and Federal and state regulatory law override the code.

2.3.3 Regulatory Agencies

Regulatory agencies affect the information infrastructure in many ways. The FCC is an independent regulatory agency established to regulate the telecommunications industry. The DoJ has a regulatory role in the telecommunications industry in the enforcement of antitrust laws. Other independent agencies, such as the Federal Trade Commission (FTC), the Interstate Commerce Commission (ICC), and the Nuclear Regulatory Commission can affect information warfare activities. For example, the Nuclear Regulatory Commission requires utilities to maintain constant communications to nuclear power plants. If isolated, the power plants are required to cease operations. Loss of this connectivity could be a serious information warfare incident. Utilities, therefore, maintain robust connectivity over private and public systems to these facilities to prevent isolation. There are several similar vulnerabilities in other industries and other infrastructures.

This report will focus on the FCC and its role in ensuring the reliability and availability of the telecommunications infrastructure.

The FCC was established by Congress as an independent regulatory agency. The FCC affects information assurance formally by issuing orders regulating the telecommunications industry and informally through generating consensus and exchanging information. The Communications Act of 1934, as amended, does not assign the FCC a national security role. It is responsible for ensuring the reliability of the Public Switched Network (PSN). Inasmuch as reliability and availability depend upon security, the FCC can influence PSN security. After the large-scale PSN outages in 1990, the FCC issued reliability regulations which, though limited in scope, levied reporting requirements on long-haul carriers and established the NRC to study and report on PSN reliability.

Effective April 6, 1992, the FCC added Section 63.100 to its rules requiring common carriers (local exchange and interchange carriers) to promptly notify the FCC of any outage that is 30 minutes or more and that potentially affects 50,000 or more customers. Subsequent rule changes require telephonic follow-up to record copy notification of FCC Watch Officers. FCC Watch Officers are located in Washington, DC, and Grand Island, NE.

The NRC is a Federal advisory committee consisting of senior telecommunications industry representatives and federal, corporate, and private customer representatives. The National Communications System (NCS) is represented on the Council. The NRC studies PSN outages and reports its findings. The results indicate that, historically, backhoes have been the principal enemy of the PSN. The report resulted in the "Call Miss Utility" publicity campaign and consideration by Congress toward levying criminal penalties for negligence in digging. The NRC continues to exchange information and consider PSN reliability issues.

Through forums such as the NRC, NSTAC, and other advisory committees, the government can influence cooperation within industry and identify priorities to senior industry representatives. Continuing deregulation of the telecommunications and information services industry will make these forums more critical in the future.

Further information on the FCC and NRC can be found in Appendix A.

2.3.4 Export Control

The Department of State (DoS) and the Department of Commerce (DoC) share authority for export control. The Arms Export Control Act of 1968 makes the DoS responsible for the export of items which are primarily for military use. The DoS maintains the International Traffic in Arms Regulations (ITAR) and a Munitions List. Items on the list require a DoS license for export; licenses are granted on a case-by-case basis. The act charges the DoD with providing recommendations to the DoS. The Export Administration Act of 1979 and the Export Administration Regulations (EAR) give the DoC responsibility for export of sensitive or dual-use products, including software and scientific data. The DoC maintains a Commerce Control List (CCL) listing controlled items. There is some overlap between the CCL and the DoS Munitions List, particularly with high technology. Generally, the DoS has purview over technology exports unless it delegates responsibility to the DoC. Figure 2-3-1 depicts current responsibilities for export control.

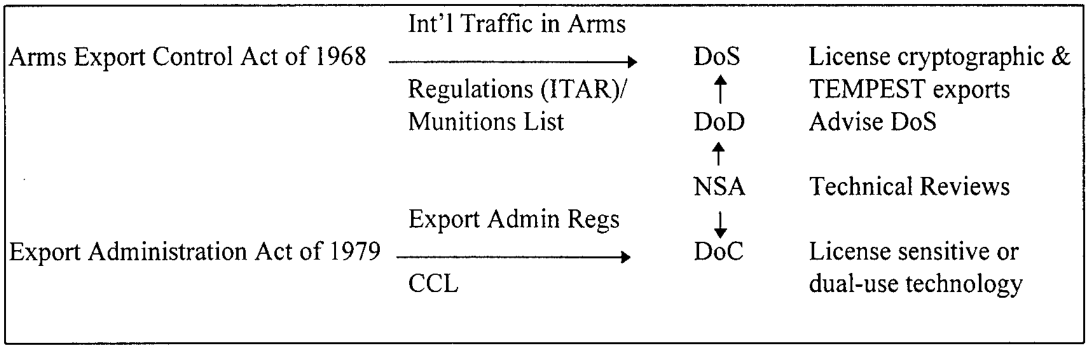

Int'l Traffic in Arms
Arms Export Control Act of 1968
DoS
License cryptographic & TEMPEST exports
Regulations (ITAR)/ Munitions List
DoD
Advise DoS
NSA
Technical Reviews
Export Admin Regs
Export Administration Act of 1979
DoC
License sensitive or dual-use technology
CCL

Figure 2-3-1. Export Control Responsibilities

Export of cryptography is a very controversial issue. In attempting to resolve the controversy, policy makers must consider national security, foreign policy, and national and international market forces. It is unlikely that export control responsibilities will change as a result of this controversy.

Figures 2-3-2 through 2-3-4 summarize the purpose and assigned responsibilities of Executive Order 12333, United States Intelligence Activities; Executive Order 12356, National Security Information; and Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions. Summaries of other relevant Executive Orders are provided in the form of annotated bibliographies in Appendix B, References.

EXECUTIVE ORDER 12333
UNITED STATES INTELLIGENCE ACTIVITIES
December 4, 1981
Purpose, Assigned Responsibilities and Functions

Purpose: Ensure the President and National Security Council are provided with necessary information to base decisions concerning foreign, defense, and economic policy and the protection of United States national interests from foreign security threats. Special emphasis should be given to detect and counter-espionage directed against government, corporations, establishments, or persons.

Restrictive Clauses:

- Agencies will not use electronic surveillance techniques except in accordance with procedures established the Attorney General.
- CIA cannot engage in electronic surveillance within the United States except for the training, testing, or as countermeasures to hostile electronic surveillance.
- Counterintelligence definition specifically excludes communications security activities.

Assigned Responsibilities and Functions:

Secretary of Defense:
- Executive Agent for signals intelligence and **communications security of the Federal government.**
- Collect military foreign intelligence and counterintelligence.
- **Provide for the timely transmission of critical intelligence within the U.S. government**.
- **Protect the security of Department of Defense installations, activities, property, information** and employees by appropriate means...

National Security Agency:
- Establish and operate an effective organization for signals intelligence.
- **Execute Executive Agent responsibilities for communication security of the Federal government**
- Conduct research and development in signals intelligence and communications security.
- Conduct foreign cryptologic relationships.

Foreign Intelligence Elements of the Armed Forces:
- "Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI."

Department of Energy:
- When requested, support NSA communications security activities.

Director of Central Intelligence:
- Primary advisor to President and NSC on national foreign intelligence.
- Develop objectives and guidance for the intelligence community.
- **Advise Secretary of Defense concerning communications requirements of the intelligence community.**
- Conduct special activities approved by the President.

Figure 2-3-2. Executive Order 12333

Department of State:

- Overtly collect information relevant to foreign relations.

Department of Treasury:

- Overtly collect foreign financial and monetary information.

Federal Bureau of Investigation:

- "Within the United States conduct counterintelligence and coordinated counterintelligence activities of other agencies..."
- Support communications security activities of the Federal government when requested by the Director of NSA.

Agencies of the Intelligence Community:

- May provide specialized equipment, technical knowledge, or assistance of expert personnel to support law enforcement activities.

Figure 2-3-2. Executive Order 12333 (Continued)

EXECUTIVE ORDER 12356
NATIONAL SECURITY INFORMATION
April 1, 1982
Purpose, Assigned Responsibilities and Functions

Purpose: Prescribes a uniform system for classifying, declassifying, and safeguarding national security information. The order recognizes "that it is essential that the public be informed concerning the activities of its Government, but" certain national defense and foreign relations information must be protected. It specifies the classification levels, authorities, delegation authorities and rules for declassification and downgrading of this information. "Information" is defined as any information or material, regardless of its physical form or characteristics. The order does not address information systems security.

Assigned Responsibilities and Functions:

National Security Council:

- Provide overall policy direction for the information security program.

Administrator of General Services:

- Responsible for implementing and monitoring the program.
- Delegate these functions to the Information Security Oversight Office.

Information Security Oversight Office:

- Develop directives for the implementation of this order.
- Oversee compliance and implementation.
- Conduct on-site reviews.

Federal Agencies:

- Promulgate implementing regulations.
- Appoint a senior agency official to administer its information security program.

Figure 2-3-3. Executive Order 12356

EXECUTIVE ORDER 12472
ASSIGNMENT OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS TELECOMMUNICATIONS FUNCTIONS
April 3, 1984
Purpose, Assigned Responsibilities and Functions

Purpose: To provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions.

General Provisions:

- OSTP and the NSC have primary responsibility for implementing this order. They will consult with OMB, FEMA, DoC, DoD, and FCC as appropriate.
- This order establishes the National Communications System (NCS) consisting of the telecommunications assets of the agencies represented on the NCS Committee of Principals (COP). The COP will consist of federal departments, agencies, and entities designated by the President which lease or own telecommunications facilities of significance to national security or emergency preparedness (NS/EP).
- The order assigns wartime and non-wartime emergency functions.

Assigned Responsibilities and Functions:

<u>National Security Council</u>:

- Policy direction for the exercise of war power functions of the President.
- Advise and assist the President in policy, plans, programs, and standards within the Federal government for the identification, allocation, and use of the Nation's telecommunications resources by the Federal during crisis or emergency.
- Policy and oversight for the mobilization of commercial, government, and private telecommunications resources, the NCS, and Federal agency implementation of this order.

<u>Office of Science and Technology Policy</u>:

- Direct the exercise of the war power functions of the President.
- Advice, guidance and assistance to the President and Federal agencies responsible for the provision, management, or allocation of telecommunications resources.
- Establish a Joint Telecommunications Resources Board.
- Recommend to the President on testing, exercising, and evaluating NS/EP capabilities.
- Recommend to the President NS/EP radio spectrum priorities.

<u>Secretary of Commerce</u>:

- Develop radio spectrum plans for Federal government use during crisis or emergency.

<u>Secretary of Defense</u>:

- Serve as the Executive Agent of the NCS.
- Designate a Manager of the NCS.
- Plan, operate and maintain telecommunications services for the National Command Authorities (NCA).
- Ensure NSA plans for security and protection of NS/EP telecommunications.

<u>Secretary of State</u>:

- Plan and provide for a reliable and secure Diplomatic Telecommunications System.

Figure 2-3-4. Executive Order 12472

National Communications System (NCS):

- Assist the President, National Security Council, Office of Science and Technology Policy, and Office of Management and Budget plan for NS/EP communications for the Federal government.
- Serve as focal point for joint industry-government planning and operations.
- Establish a joint industry-government National Coordinating Center.

NCS Committee of Principals:

- Serve as a forum for the review and evaluation of ongoing and prospective NS/EP telecommunications programs.
- Serve as a forum for each agency to report on their ongoing or prospective telecommunications programs in support of NS/EP.

Manager of the NCS:

- Recommend to the Executive Agent and COP an evolutionary architecture, plans to remove or minimize technical impediments to interoperability of government owned or leased telecommunications systems and test and exercise programs.
- Chair the NCS Committee of Principals and provide staff support.
- Implement approved plans or programs.
- Serve as the joint industry-government focal point including technical information concerning the NS/EP telecommunications requirements of the Federal government.

Federal Emergency Management Agency:

- Plan, operate and maintain telecommunications services and facilities to support its emergency management responsibilities.
- Advise State and local governments on NS/EP.
- Provide policy and management oversight of the Emergency Broadcast System.

Central Intelligence Agency:

- Plan, operate, and maintain telecommunications services adequate to support assigned responsibilities and disseminate intelligence within the Federal government.

General Services Administration:

- Ensure Federally owned and managed telecommunications systems meet NS/EP requirements.

Federal Communications Commission:

- Ensure plans for NS/EP communications services are in the public interest, convenient, and necessary.
- Coordinate NS/EP activities with NCS.

Federal Agencies:

- Provide NS/EP requirements, funding, and reports to the Manager of the NCS.

Figure 2-3-4. Executive Order 12472 (Continued)

This page intentionally left blank.

2.4 POLICY ENVIRONMENT

Particularly as it applies to a government body, policy is defined as a high-level overall plan or course of action intended to influence and determine decisions, actions, and other matters. Policy guidance and documents are generally less permanent than regulatory documents, and carry neither the weight nor the force of law. Policy generally applies to a subset of the population, although universal application is not excluded.

Currently, there is no national policy on information warfare; however, a body of guidance is being created in the Executive Branch. Several policy boards, committees, and working groups have been established to address security policy for the government.

Specific issues which fall into the realm of information warfare have been addressed in policy documents as the need has arisen. The DoD has produced most of these policy documents. Other regulatory agencies providing policy include the DoC, the DoJ, and the Department of the Treasury (DoTreas).

Issues relating to information warfare are perceived in various ways at the national level. The DoD clearly has an interest in promoting a coherent, national policy and strategy for information warfare. Other Federal Departments and Agencies with a stake in information assurance may have differing perspectives on how to implement information assurance goals. For example, while the missions of Justice and Treasury are very different, both departments are concerned with the protection of information. Their purpose in protecting that information will be driven by dissimilar motivations and mission requirements, different sets of data sensitivity and criticality, and a great variety of threats and vulnerabilities.

Another key factor which contributes to the complexity of the issue of policy at the national level is the dynamic nature of technology. We have already seen the rapid confluence of information and telecommunications. We have seen the emergence of terms, such as information superhighway and global/national/defense information infrastructure. The evolution of technology, and its concurrent influence on the missions of Federal Departments and Agencies, must be closely observed; appropriate responses in the form of intelligent strategies and policies, cogent investment decisions, and responsive implementation plans must be made. One thing is certain—the technological environment and its impact on information warfare will continue to be dynamic. Policy must be crafted in such a way that changes in technology do not result in major policy changes.

2.4.1 Overview of Existing Policy

The policy documents within the Executive Branch which may influence the creation of policy for information warfare in DoD are summarized in Table 2-4-1. (For a listing of key policy documents, see Appendix B, Policy Document Index.) Most of these documents have been produced within the DoD, reflecting the DoD's greater sensitivity to information warfare. Table 2-4-1 is a representative sample of documents that relate to any aspect of the transmission, storage, or protection of information. Numerous documents dealing with such topics as personnel security, physical security, communications doctrine and procedures, and security hardware have been excluded. With few exceptions, the handling of intelligence-related information has also been excluded.

Table 2-4-1. Information Warfare Policy Document Summary

POLICY DOCUMENTS	
Number	Type Document
2	Presidential Directives
4	National Security Directives/Decision Directives
7	National Communications Security Committee Policies
6	OMB Circular
	Federal Information Resources Manual (IRM)
33	OSD, Defense Management Review Decisions, Directives, Standards, Regulations, Manuals, Handbooks, Indexes, and Instructions
1	CJCS, National Military Strategy Document, Memoranda of Policy, Instructions, Joint Publications
1	NSA Policy
9	Army Regulations
15	Navy Instructions
2	Marine Corps Orders/Publications
11	Air Force Regulations and Instructions
	Note: Executive Orders were discussed in Section 2.3, Regulatory

2.4.1.1 Executive Branch Policy

The lack of National-level policy on information warfare is a source of concern for many, particularly for the DoD. There is debate across the Federal Government as to whether or not a national policy for information warfare is required, how it should be defined, what its components and boundaries are, and whose responsibility it should be. It is a complex issue at the very least, encompassing many legal and regulatory concepts, and confronting such constitutionally-guaranteed rights as individual privacy.

At the Presidential level, policy has been expressed in such instruments as NSDDs, and issuances of the National Security Telecommunications and Information Systems Security Committee and its predecessor organizations, the National COMSEC Committee and the National Telecommunications and Information Systems Security Committee. For example, NSD 42 stated, as a matter of policy, that "national security systems shall be secured by such means as are necessary to prevent compromise, denial, or exploitation"; established an executive agent and a national manager to implement objectives and policies; and redefined the charter of the NSTISSC to include developing operating policies, procedures, guidelines, instructions, and standards.

Another initiative being fostered at senior levels of the Executive Branch is the support for the so-called Information Superhighway. Vice President Gore is spearheading administration efforts under the Information Infrastructure Task Force (IITF). The information infrastructure of the future will be a key component of any information warfare strategy or policy, whether at the national level, or in the DoD.

A major factor in the handling of information is the delineation of responsibilities by the Computer Security Act of 1987 for classified and unclassified information. Although the DoD has traditionally placed itself at center stage in the ongoing debate regarding information handling, the act very clearly assigned responsibility for policy formulation for sensitive unclassified information to the DoC. The NIST was delegated the responsibility for sensitive unclassified standards and guidelines. The DoD retained its role for classified information.

A cornerstone document to the security of information is OMB Circular A-130, Security of Federal Automated Information Systems. Revisions to the original document have been made over the past two years. The most recent proposed revision of Appendix III addresses security. The transmittal letter contains the following language, which is a reflection of current thinking at senior levels in the Executive Branch: "This proposal is intended to guide agencies in securing information as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls. The proposal would also better integrate security into program and mission goals, reduce the need for centralized reporting of paper security plans, emphasize the management of risk rather than its measurement and revise government-wide security responsibilities to be consistent with the Computer Security Act."

In May 1993, the Secretary of Defense and the Director of Central Intelligence established a Joint Security Commission (JSC) to examine the processes used to formulate and implement security policy in the DoD and the Intelligence Community. In executing its charter, the JSC was guided by the following needs: flexible policies to match threats; consistent and cost-effective policies; fair and equitable treatment of all Americans; and affordable security. The Commission saw current security practices and procedures as complex, costly, and fragmented, and a "profusion of policy formulation authorities" with overlaps and sufficient differences "to create inefficiencies and cause implementation problems." The JSC observed that "the policies and standards upon which the Defense and Intelligence Communities base information systems security services were developed when computers were physically and electronically isolated. As a result, policies and standards:

- Are not suitable for the networked world of today . . .
- Were developed based on a philosophy of complete risk avoidance and so do not deal effectively with information systems security as part of a balanced mix of security countermeasures . . .
- Do not provide the flexibility needed to address the wide variations among systems in use today and planned for tomorrow.

- Do not differentiate between the security countermeasures needed within and among protected network enclaves and those needed when information must travel to and from less protected or unprotected parts of the infrastructure.
- Are only beginning to combine computer science and public key cryptography . . .
- Are not capable of responding . . . to dynamically evolving information technology."

The JSC recommended the creation of "a joint DoD/DCI security executive committee, and that the committee oversee development of a coherent network-oriented information systems security policy for the Department of Defense and the Intelligence Community that also could serve the entire government." The structure which was put in place was shown in Figure 2-1-2, U.S. Security Policy Board.

The 12-member U.S. Security Policy Board was created under the National Security Council by PDD 29. Below the Board were established a 26-member Security Policy Forum (composed of representatives of other Federal agencies and departments) and a 5-member Security Policy Advisory Board with civilian membership. The Board has subordinate working groups to address such subjects as personnel security, physical security, information classification, system security, training, and policy integration.

The existence of and the work of the Board is presently encountering resistance from those who see an overbearing presence from Defense interests, and an attempt to institute closer relationships between the classified and unclassified environments. The future of the Board and its work is the subject of vigorous debate.

The DoD is also pressing forward with its desire to create a national policy for information warfare. A draft Presidential Review Decision (PRD) is being circulated and staffed.

2.4.1.2 Department of Defense Policy

Considerable effort has been undertaken within OSD and the services to move forward in the information warfare area, including the creation of policy documents. These documents have been written to fulfill the primary mission of DoD, i.e., the execution of national military strategy as directed by National Command Authority. A primary source is the National Military Strategy Document for FY94-99, dated 19 June 1992, with its various annexes, most notably Annex C, Command, Control, Communications, and Computer Systems. This annex provides programming guidance and priorities to support the force structure required to execute the national military strategy and serves as support documentation for the core C4 capabilities identified in the Defense Planning Guidance.

The Secretary of Defense and OSD have published Regulations, Directives, Manuals, Handbooks, and Instructions which relate either directly or indirectly to information warfare. Most notable among these is DoD Directive TS3600.1, Information Warfare. This directive establishes DoD information warfare policy and assigns responsibilities. It provides the basis for developing policy within DoD and in the services and directs acquisition of systems to meet operational requirements. It specifically assigns responsibility, for example, to the Assistant Secretary of Defense, for C3I as the primary point of contact for information warfare within DoD; the Director, NSA, for information purposes in matters relating to technology and system development; and, the Director, DISA, for the protection of the Defense Information Infrastructure (DII). DoDD TS3600.1 is currently being revised. Protection of the DII is the basis for a Memorandum of Agreement between DISA and NSA concerning the Defense-Wide Information Systems Security Program (DISSP).

Secretary of Defense Cheney approved policy documents known as Defense Management Review Decisions (DMRDs), which have relevance to information warfare and information systems. The most well known of these is DMRD 918.

The Chairman, Joint Chiefs of Staff (CJCS), has similarly issued Instructions, Memoranda of Policy (MOPs), and Joint Publications. Joint Publication 1, Joint Warfare, refers to the "information differential." CJCS MOP 30, Command and Control Warfare (C2W) provides joint policy and guidance for both offensive and defensive aspects of C2W.

2.4.2 Military Department and Service Policies

The military departments and Services have been busily engaged in developing and implementing of policy for information warfare. Although lacking comprehensive guidance from higher authority, emerging service policy, doctrine, and implementing instructions generally refer to DoD Directive TS3600.1 and CJCS MOP 30.

Efforts of the services appear to be proceeding in the same general direction. There are universal concerns for such items as national-level policy, drafting of doctrine, establishing executive agency responsibilities and an operating structure, staffing, integration of information warfare into traditional missions, acquisition, and training.

The exploration of military department directives in detail is beyond the scope of this paper. Suffice it to say that CJCS policy action on information warfare would impact heavily on Service review and conformance efforts.

2.4.3 Implementation Standards, Guidelines, and Procedures

Within the Executive branch of government, there exists a large body of standards, guidelines, and procedures designed to implement policy. As instruments of policy, this guidance is essential to ensure adherence to both the letter and the intent of policies from higher authority. In fact, the traceability of guidance and procedure is made not only to policy, but frequently to law.

These standards, guidelines, and procedures generally fall into one of the categories shown in Table 2-4-2. It is not within the scope of this paper to explore the details of the implementing guidance. For a listing of key implementation guidelines, standards, and procedures, see

Appendix B, Implementation Guidelines, Standards, and Procedures Index. The index contains a thorough representative sample of documents.

Table 2-4-2. Implementation Guidelines, Standards and Procedures

IMPLEMENTATION GUIDELINES, STANDARDS, AND PROCEDURES	
Number	Type Document
24	National Communications Security (COMSEC) Instructions (NACSIs), Information Memoranda (NACSIMs), and Emanations Memoranda (NACSEMs)
63	National Telecommunications and Information Systems Security Committee/National Security Telecommunications and Information Systems Security Committee (NTISSC/NSTISSC) Issuances
4	Office of Management and Budget Bulletins
	Director, Central Intelligence Directives
36	National Computer Security Center (NCSC) Rainbow Series
33	NIST Special Publications
146	Federal Information Processing Standards Publications (FIPSPUBS)
7	DIA Manuals
2	Compartmented Mode Workstation (CMW) Publications
6	COMSEC Program Publications
9	TEMPEST Program Publications
4	Other Security-relevant Government Publications

2.5 EMERGING TECHNOLOGIES

Emerging technology has had, is having, and will continue to have a profound impact on both offensive and defensive information warfare. Emerging technology involves all stages in the processing, transmission, storage, encryption, and protection of information. Technology has also advanced in related areas such as physical security, access controls, and audit techniques. Technology solutions are not limited to either hardware or software, but cover the entire spectrum of potential solutions. In many cases, there is a continuous spiral of development as countermeasures are developed to mitigate vulnerabilities, new methods of attack are discovered, and yet additional countermeasures are required. Many technology solutions have the potential of being used for illicit purposes; that fear has recently been expressed with reference to the Security Administrator's Tool for Analyzing Networks (SATAN).

Governments, individuals, and corporations rely more upon information. As Toffler notes in his book, *The Third Wave*, we have become an information-based society. As information becomes more available, and reliance grows, the effects that could result from the loss of the information become more serious. People and organizations rely upon technology for their daily activities. If a serious and coordinated attack is made upon telecommunications assets, there will be serious effects on the general public as well as the military. The military's ability to conduct effective operations will also be seriously impaired.

This section addresses highlights of emerging technology topics as they apply to the NII. Technologies that are specifically related to battlefield modernization and tactical warfare are predominantly classified, and are not addressed. Emerging technologies are being fostered by such efforts as the Joint Warfighters Capability Assessment (JWCA) and research and development in technologies which potentially have long-range information warfare applications. Examples of emerging technologies include the following: network encryption; network sniffers; network watch dogs; packet filtering using firewalls and routers; authentication techniques; efficient communications protocols with increased throughput; broadband communications; and wireless communications. The remainder of this section will address the key security triad of confidentiality, availability, and integrity (in terms of authentication, encryption, communications, and firewalls), and present a brief discussion of the electronic battlefield.

2.5.1 Confidentiality/Availability/Integrity of Information

Our society, in general, has greater reliance upon information and technology than others. The NII (a subset of which is the DII) is enabled by this technology. Disruptions to the infrastructure, as we have experienced through both natural and manmade disasters, have highlighted our critical reliance on information. During these disruptions, both the psychological effects and the incredible cost of deprivation of information have been felt. Emerging technology has the potential to provide some relief. Minimization of effects of disruptions of the infrastructure will require improved information protection.

Information protection is considered in terms of the confidentiality, availability, and integrity of information being handled within the infrastructure. It requires proper implementation of security features appropriate for individual environments, such as passwords, firewalls, or other countermeasures. Many technology advances are developed in reaction to an identified problem.

Authentication and encryption are two areas that are evolving quickly on the international level. While these techniques may provide effective measures to ensure confidentiality and/or integrity of information, they are rendered useless by a denial of service attack on the information infrastructure. Denial of service, or denial of the availability of information, vulnerabilities provide greater opportunities for an adversary attack; it is consequently exceedingly difficult to provide ironclad countermeasures against a denial of service attack. A comprehensive risk analysis and implementation of recommended countermeasures are essential to mitigate threat-vulnerability exposure.

2.5.1.1 Authentication

Authentication is the verification of the identity of an individual or the source of information. In its simplest form, authentication can be thought of in terms of traditional passwords or a Personal Identification Number (PIN). Authentication of identity can also be achieved by other devices, such as tokens, smartcards, or biometric devices which can be attributed uniquely to one individual. Authentication of the source of information can now be demonstrated through such techniques as the digital signature.

The use of passwords is the simplest method of authentication to implement, as well as being the most acceptable to the general public. But because of applications that can guess and steal passwords (such as the DoD has experienced during attacks through the Internet) and poor password management on the part of users, the use of passwords to provide secure authentication has been severely compromised. The use of one-time passwords, or similar one-time, encrypted authentication techniques may provide a more secure protection mechanism.

Tokens may also be used to authenticate an identity. The individual must present a card to the system and enter a password, as in the mechanism used for an Automated Teller Machine (ATM). Biometric techniques are by far the most exotic and expensive form of authentication. Their advantage is that they are relatively accurate, and, unless the data base is compromised, eliminate the vulnerability associated with a compromised password or a lost token. In almost all cases, the inaccuracies yield false negative responses, rather than false positive responses, thus erring on the side of strengthened security. Common biometric authentication techniques include fingerprinting, hand measures, voice identification, and retinal scans.

Digital signatures provide an authentication mechanism that a sender and a receiver of a message can use to verify the identity of the sender of a message, and thus the message integrity. Digital signatures use public key cryptography to associate the sender uniquely with the message.

2.5.1.2 Encryption

Encryption is the transformation of data into a form unreadable by anyone without the appropriate decryption key. Encryption allows secure communications over an otherwise unsecure channel. Many products are being implemented that address encryption and/or secure communications using password systems, cards, single-use keys, public key systems, and private/secret key systems.

Some of the encryption systems currently available or being developed include S/KEY, Kerberos, RSA (named after its creators, Rivest, Shamir, and Adleman), Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP), Digital Encryption Standard (DES), Public Key Cryptography Standards (PKCS), and SKIPJACK. To understand the impact these systems may have on information warfare, it is important to understand the difference between public key and private/secret key systems. Traditional cryptography is based on both the sender and the receiver of a message knowing and using the same private/secret key. A significant problem with private/secret key systems is the secure distribution of the key. Public key systems try to alleviate this key management problem. In a public key system each person has two keys, a public key and a private key. The public key is used to encrypt messages and the private key is used to decrypt messages. In this way the private key is never transmitted across the network. Public key systems are often significantly slower than private/secret key systems. Combinations of these systems can be used where the public key system is used to encrypt a private/secret key which is used to encrypt a message. Using this methodology, the identity of a sender can also be authenticated while the data is protected.

S/KEY is a single-use password authentication system developed at BELLCORE and publicly available on the Internet. The purpose of S/KEY is to prevent network sniffing applications from discovering user passwords. A secret password of the client is used with a seed from the host to generate a sequence of single-use passwords. Only the derived, one-time password crosses the network.

Kerberos is an authentication system designed to prevent password detection within a Kerberos environment or among hosts all fully supporting the Kerberos protocol. Kerberos is based on DES symmetric key encryption and uses a trusted host as an independent source of key verification. The Kerberos trusted host or server contains all the secret keys and must be physically secure. If the host is compromised, so are all of the secret keys.

There are also asymmetric encryption systems such as RSA. SPX is an experimental system that uses RSA. SPX depends on each party having a certifying authority. It uses digital signatures that consist of a token encrypted in the private key of the signing entity and that are validated using the appropriate public key. The public key is obtained under the signature of the trusted certification authority. Parts of the authentication exchange are encrypted to prevent a replay attack.

PEM is an Internet mail standard that has been designed and proposed but not yet officially adopted. It was created to provide secure e-mail and works with current e-mail formats. Currently PEM explicitly supports only DES message encryption and supports both DES and RSA for key management. Trusted Information Systems, Inc. (TIS) has released an implementation of PEM that is intended for the use of individuals, not commercial use. There is no cost for the TIS software.

PGP system is based on RSA but does not require a certifying authority. PGP was developed by Phil Zimmerman who provided it freely, resulting in international distribution. It is currently being debated whether PGP contains copyrighted material and whether PGP falls under the regulations which govern the exporting of cryptographic technology. PGP for individual use is available for the DOS, Mac, UNIX™, Amiga, Atari, VMS, and OS/2 platforms and has Italian, Spanish, German, Swedish, and Russian foreign language modules available. PGP is available via anonymous file transfer protocol (ftp) from sites in the United States, Germany, Sweden, Spain, Canada, United Kingdom, Italy, Finland, Australia, Netherlands, and New Zealand. PGP is also available commercially from ViaCrypt, but this version is not available for export from the United States.

DES is an encryption block cipher defined and endorsed by the U.S. Government. DES is a secret-key, symmetric encryption system. Symmetric key encryption means that the same key is used for encryption and decryption. DES hardware and software export from the United States is strictly regulated by the DoS and NSA. However, the DES algorithm is currently in use worldwide.

PKCS is a set of standards for implementation of public-key cryptography issued by RSA Data Security, Inc., in cooperation with a computer industry consortium. PKCS is compatible with PEM but extends beyond it to handle binary data. It supports RSA, DES, and Diffie-Hellman key exchange.

SKIPJACK, the algorithm used by the Clipper chip, is a classified encryption/decryption algorithm designed by NSA. It is designed with a law enforcement access field (LEAF) which enables an authorized law enforcement official to decrypt the data. Reviews of SKIPJACK show it to be significantly more robust (more resistant to breaking) than DES. However, there is significant public concern about the law enforcement access and about the possibility of NSA being able to decrypt messages.

Key escrow involves an escrow agent maintaining a copy of an encryption key that can decrypt otherwise secure data. Law enforcement agencies need to decrypt messages, because otherwise well-financed criminal organizations can secure their communications against monitoring by law enforcement agencies. Key escrow provides for messages to be secure from all unauthorized readers, except for valid law enforcement authorities. This concept is a source of significant public controversy, because there is strong public sentiment against the Government being able to compromise data that the public perceives to be secure. An additional controversy arises when exportation of key escrow is required. U.S. companies attempting to sell computers to foreign entities would be required to sell them with the key escrow feature, which would make the product undesirable to the foreign buyers. Because there are many other methods for encrypting data, the foreign buyers are not limited to considering U.S.-made products if they desire security features.

The export restrictions placed on related hardware and software inhibit widespread implementation of U.S. manufactured authentication and encryption systems. These restrictions discourage commercial application developers from including encryption systems in their products. Encryption is also illegal in some countries.

2.5.1.3 Communications

There will soon be a proliferation of high-volume data communications exchange systems. Industry is driving the market and technological advances in increased communications bandwidth. The new technologies that are facilitating higher rates of data communications include Synchronous Optical Networks (SONET), Asynchronous Transfer Mode (ATM), Frame Relay, Broadband Technologies, and Integrated Services Digital Network (ISDN). While these protocols are very different in implementation, they all allow for a dramatic growth in bandwidth. ISDN is primarily intended to provide relatively high data transfer rates to small businesses and home computers, and the other protocols are intended for use in Wide Area Networks. Care must be exercised in employing these technologies, as the degree to which security features have been considered and implemented will vary, and vulnerabilities will exist.

SONET is a fiber based ring technology that, while offering significant bandwidth, is vulnerable to interception. Data messages are transmitted intact throughout the ring from one node of the network to another. If a node determines that the message is not intended for that particular node, then it will pass the message on to the next node of the ring. The problem is that every node on the ring could read or intercept data intended for another node, allowing for the potential compromise of all data on the network.

ATM uses cell-relay technology. A cell is a fixed-size, fixed-format packet. Cell and Frame Relay technologies are protocols that break up a message into many packets and transmit each packet according to the most efficient route. Packets from the same message might have totally separate routes, and it is the responsibility of the receiving node to reassemble all packets into the original message. These packet-switched protocols allow for great redundancy and survivability. A significant portion of a packet-switching network must be disabled for communications to be lost. In spite of some inherent protection, ATM/SONET networks can be disrupted and data can be compromised. Indications are that early commercial and government implementations of ATM/SONET are not very secure.

ISDN is intended for high data transfer rates for low usage communications links. ISDN services are provided by the Regional Bell Operating Companies, and use local telephone lines. The protocol allows for two separate streams of data: a voice stream and a data stream. Separate data streams allow for simultaneous activities. Since ISDN services are dependent upon the Public Switched Network (PSN), they are susceptible to the same types of compromises that are faced by all other data transmitted over telephone lines.

2.5.1.4 Firewalls

Firewalls filter network traffic and preventing undesirable traffic from reaching protected computers. Firewall use is increasing and will continue to do so. The firewall technology can effectively secure networks from intrusion in many cases. However, different firewall vendors provide different levels of protection. Despite the potential for compromises, firewalls can provide one of the more effective protection mechanisms, when they are properly implemented.

Firewalls have several disadvantages. The firewall is a bottleneck for network traffic and a single point of failure for the local network. If a firewall does not function, all connectivity may be lost. Additionally, firewalls are not very versatile when it comes to providing additional services, such as allowing for new communications protocols. Effective firewalls also limit services to individuals, limiting system functionality and frequently limiting usability. Many organizations struggle with the security versus usability conflict.

2.5.2 Electronic Battlefield

The proliferation of information is also heading to the battlefield. All U.S. military units rely upon information technologies for basic functionality. For example, the Global Positioning System (GPS) has improved the efficiency of military operations and weapons employment.

Not only are forces in the field better informed, they are also better equipped. The miniaturization of technology provides forces with portable computers and communications systems, allowing for the modification of plans, tactics, and strategies in real time.

New problems of compromise arise as portable technology is integrated into the battlefield. Additionally, equipment and technology are placed closer to the conflict, which could provide access to U.S. communications circuits, and thus to critical strategic and tactical information. Two separate methods of minimizing the ill effects of enemy capture should be considered: authentication mechanisms and tamperproof containers or destruction mechanisms. Authentication mechanisms that minimize exploitation of captured equipment must be considered.

The electronic battlefield will create new training challenges. Our forces must be trained to operate efficiently both with and without new technology. They must be able to utility fully the information provided by technology, but they must also continue to operate if their equipment is rendered useless. Training must not ignore basic skills, even when the environment relies upon technology.

2.6 ADVERSARY CAPABILITIES

Information warfare has both offensive and defensive aspects. Adversary issues play a part on both sides of the information warfare equation. In order to mount an effective offense, the adversary must be understood in sufficient detail. This entails "knowing thy enemy" in terms Sun Tzu would appreciate, i.e., knowing the infrastructure and decision process in detail. DIW requires not only some knowledge about potential enemy information warfare capabilities, but also detailed understanding of one's own infrastructure and vulnerabilities. This clearly implies knowing more about the infrastructure and its interconnectivity, both here and abroad. But it also implies an understanding of the potential for new threats, such as software or hardware attacks on information systems.

Some new fundamentals apply to this warfare area. Much of the system architecture we might use in a war might be shared...some may even be shared with an adversary. It must be expected that any information system that is not totally closed from the outside world is vulnerable to compromise. Intruders have been able to crack many technologies that have been developed, and it must be expected that they may compromise any technologies that will be developed. In such an environment, rapid reconstitution may be critical. Intruders do not have to exploit the technology if they can bypass the technology through non-technical means, or if disruption is the goal rather than exploitation. Many of the information warfare issues and questions are familiar, but the pace of change and scale of the problem is new. Moreover, the state-of-the-art in this technical area is in the commercial world—not in DoD.

Information warfare attacks may be made upon information systems, but they may not be made with the sole intent of disabling the military information infrastructure. The DoD operates within a larger national and international infrastructure of information systems. This infrastructure supports many functions within society, and those functions (not the supporting information infrastructure) may be the ultimate targets of information warfare actions. Thus, attacks may be aimed at disabling economic activities or safe air traffic control or power distribution in ways which constrain national security. The defensive issues may be outside the purview of DoD, but are not beyond the scope of potential information warfare approaches to warfare and the concomitant requirement for information regarding adversary capabilities. Clearly, for DoD approaches to DIW, knowledge of potential adversary functional capabilities must be collected and analyzed.

Finally, the legal and regulatory environment in which we address potential adversaries—particularly in peacetime—has not kept up with the rapid change which technology has generated. Thus, the U.S. Government faces obstacles in its efforts to constrain adversary information warfare approaches.

2.6.1 Elements of Information Warfare

> "*Elements of Information Warfare:*
>
> • *Design and leverage of one's own information systems to provide decision makers with actionable information;*
>
> • *Protect those information systems from disruption, exploitation and damage; and*
>
> • *Employ offensive information warfare techniques such as deception, electronic warfare, and advanced technologies to deceive, deny, exploit, damage, and/or destroy adversary information systems.*"

Figure 2-6-1. 1994 Defense Science Board Summer Study Quote

Inherent in the Defense Science Board's description of the attributes of information warfare, there are clearly two aspects of that effort: defense of U.S. systems and capabilities, and offense against a potential opponent. On the defensive side of the equation, the rapid pace of change in information technology and systems continually changes the nature of U.S. vulnerabilities substantially. This changing nature poses many questions: Where does defense need to adapt? What might DoD and Service responsibilities be? What is happening to Service vulnerabilities, and to those of the operating forces (under the auspices of the Commanders In Chief (CINCs))? On the offensive side, change also brings a long list of questions. Even the old questions may have new answers in the changed environment. In order to plan and execute military information warfare offensive operations, we must not only understand in detail the opponent's information infrastructure. We must also thoroughly understand the adversary's whole decision process.

Information warfare creates comprehensive new requirements for intelligence. Offensive and defensive IW intelligence requirements are closely linked. Adversary capabilities and vulnerabilities are critical to both offensive and defensive operations. The traditional functional intelligence areas of early warning; detection; identification; mapping; and understanding the adversary, his thought processes, his perceptions, and his culture must be reexamined. Coherent strategy, both indepth and operational, for information warfare intelligence must be developed. This should not be simply a collection strategy; rather, it must also incorporate surveillance planning, data base and decision aid development, and considerations of timing and sequencing normally associated with operational planning. The strategy must address the following key issues.

The first challenge is the number and identities of potential adversaries. The United States faces a multipolar world, one in which it is much more difficult to determine who the next adversary might be and what his capabilities or vulnerabilities might be. The focus of the past fifty years on the former Soviet Union consumed a vast percentage of the intelligence resources, and at the same time lent some assurance to targeting. Today, there is a much longer list of potential adversaries, including non-state actors. A list of 20 or so possibilities adds measurably to the intelligence task, but does not capture the full spectrum of potential information warfare opponents.

After determining who the adversary might be, we must determine the adversary's current technological capabilities in the area of information systems and the actual information infrastructure. How this infrastructure interacts with others, with the international environment, and finally with the U.S. infrastructure, is a central information objective. One problem that we must address is how to represent this infrastructure and its interconnections to the U.S. planners and commanders.

Technology proliferation is a particularly significant problem in information warfare, because the commercial world is driving the state of the art in many of the key technology areas. Another issue is that of understanding the adversary's potential future capabilities. The potential proliferation of information technology amplifies the list of potential adversaries and expands their capabilities. Understanding the dynamics of information and related technology proliferation is a crucial part of understanding the threat that potential adversaries might pose.

Yet another issue relates to understanding the opponent's decision processes, command and control processes, infrastructure, and sustainment functions. This issue involves knowing everything about the adversary, from who the decisionmaker is, to details about preconceptions, decision rules, data bases, and decision support systems, key advisors, etc. It is nearly impossible for the intelligence system to supply all of the necessary details, even when focused on a single or only a few adversaries. Nevertheless, all of these details are necessary with information warfare. This issue includes the way in which the adversary might plan to use his information system. Questions of emphasis, timing, sequencing, and network effects are only a few of the factors which must be considered.

One last point should be emphasized regarding information warfare. There is a potentially significant asymmetry in employable means between the adversary and the United States. A potential opponent can often use any means technically available to penetrate and exploit or disrupt and deny U.S. information systems—in peace as well as in war. The U.S. warfighters, however, may have significant constraints placed upon them by law and regulation, limiting their actions.

These issues of adversary capabilities and potential capabilities, taken together, are the raw material of understanding how vulnerable an adversary might be to information warfare and how an adversary's capabilities may impact the United States. We must include some sense of that vulnerability in planning; we must derive and further develop adequate measures of relative vulnerability. It is currently hard to model relationships of this sort, partly because adequate measures of effectiveness do not exist. Although some elements of information warfare can be measured in input terms, and some measures of merit partially described, there are still too many unquantified or unquantifiable terms (e.g., deception, perception management, command, etc.) to permit a detailed analysis. For example, a vulnerability which cannot be attacked (because appropriate systems do not exist, or other constraints apply) is not really a vulnerability. Such a judgment implies some sense of a net assessment against one's own capabilities—but it remains hard to attach numbers to such judgments.

For the defensive information warfare planner, the above considerations are also important. However, the focus shifts to assessing how our potential adversaries perceive our vulnerabilities, and how they might intend to exploit them. Although this might be a sufficient statement of the intelligence requirement, it entails many sub-elements of details which make it a very broad requirement indeed. Questions such as how much the potential opponent knows about the U.S. information infrastructure and decision process, what technologies the opponent might couple with what skills, what he might know about U.S. perceptions, and so on are a few of these details. Furthermore, the key questions may not just focus on military capabilities and military doctrine. Information warfare by a potential opponent may have as its focus elements that go well beyond the Defense and military infrastructure. Targeting industrial or other targets is not new, but the information warfare manifestation may be particularly leveraged against non-DoD elements. This of course makes the information assurance task for the United States a very broad one, with potential for multiple government agency and civilian organization involvement. Note the comment regarding asymmetries versus the opponent supra; he may not have such a complex task of coordination.

Thus, the information warfare threat to the NII must be considered in the war of the future. While an attack on the NII might not directly affect the capability of military hardware or war fighting capability, such an attack could invisibly (or visibly) cripple the United States without a shot being fired and without direct knowledge of who the adversary may be. For example, during Desert Storm, the allied forces concentrated fire power on the Iraqi NII. This left Iraq blind to attack, crippled the Iraqi economy, and demoralized the nation. While the allied forces primarily used munitions to destroy the NII, similar attacks can be accomplished against the United States through electronic means.

2.6.2 Military Capabilities

2.6.2.1 Disruption of Communications

The military theory of the former Soviet Union included strong incentives to disrupt an enemy's ability to communicate, as a prerequisite for, or in support of, operations. More recently, in the aftermath of the Gulf War, the Russian military theorists indicate that gaining an initial information advantage is potentially war winning. Losing the ability to communicate can leave a military unit in the dark, forcing every individual soldier and unit to operate independently of others. A coordinated attack becomes nearly impossible, particularly in a rapidly changing situation. Communications are vulnerable on many levels, and attacks on all levels of communications should be expected.

Communications also can be disrupted on a national level. Communications occurring between senior national or military leaders can be critical to the execution of military operations. There are several methods that can be employed to disrupt communications at this level. For example, adversaries might be able to damage satellite communications by disabling the satellite transmission stations, by disabling satellites themselves, or by jamming, intrusion or other soft-kill mechanisms.

The U.S. military relies heavily upon the use of commercial telecommunications for all levels of communication. As will be discussed later, there are many threats to telephone lines, both nationally and internationally. A disruption in the telephone system could cause a loss of communications.

Radio transmission is a central element of military communications and may be disrupted in many ways. While large-scale jamming and disruption are not usually feasible, selective jamming is possible at critical points in operations. Additionally, attacks on stationary transmitters and relay stations should be expected from a variety of conventional and non-conventional sources. Although this is not new, some of the potential attacks may have a different character in the rapidly changing environment of global communications. There are a number of new techniques, or old techniques with new applications, which expand the spectrum of threats to communications systems.

2.6.2.2 Modification of Data

The possibility of false or misleading communications represents a very significant threat to military operations. For example, during the Vietnam War, North Vietnamese radio operators frequently impersonated U.S. soldiers to call in air strikes on U.S. targets. The Russians also practiced radio intrusion successfully against U.S. forces. In future conflicts, it may be possible for one side to modify targeting data in the other's computers. Assurance of data integrity thus becomes a key component of information assurance. Encryption will not necessarily assure data integrity, since introducing false data bits or modifying the data elements in data bases can often be done without reading the internals of messages.

As will be discussed in later sections, adversaries have connected to U.S. computer systems and modified or stolen data. Individuals, such as Kevin Mitnick, have allegedly also rerouted commercial communications lines. This technique, applied against military circuits, could allow an adversary to enter false requests for attacks. If an adversary compromises information assets by deleting correct data or adding false data, then U.S. assets may take actions that are incorrect and damaging to U.S. interests.

2.6.2.3 Cover and Deception (C&D) and Psychological Operations (PSYOP)

In the military environment, Cover and Deception (C&D) and Psychological Operations (PSYOP) have been used throughout history. U.S. adversaries, from North Vietnam to Somalia, have used information to influence U.S. policy and public opinion. In the past, the United States and its adversaries have used various techniques to influence military operations.

PSYOP and C&D have also been used to demoralize an enemy or to sway public opinion against military actions or government decisions. In many cases, effective use of PSYOP and C&D has proved to be a more powerful weapon than military actions. Defense against such an attack is difficult.

Good intelligence data can alleviate the threat posed by C&D. Nevertheless, C&D use can increase uncertainty in a commander's decisions. Uncertainty implies delay, and delay can be critical to military outcomes.

PSYOP are even harder to control. Widespread dissemination by the U.S. media and its independence vastly complicate military operations. Any information warfare strategy must take into account the press and at least address its potential impact. It will be a key component of the information environment.

2.6.3 Threats to the Information Infrastructure

There is a significant threat posed by adversaries of the United States Government to U.S. information assets throughout the world. It is generally accepted that if a single person has developed the capability to compromise an information system, then any group or individual may obtain the knowledge or services of that person. Thus, the potential threat of software or hardware attacks on computer systems must be carefully evaluated as a part of any information warfare strategy. The potential adversaries include countries and other groups (and individuals) which seem likely to have hacker-like capabilities. While traditional computer hackers do not necessarily represent a direct threat from an information warfare perspective, they provide the knowledge for U.S. adversaries to wage devastating attacks against a variety of assets. Usually, hackers are the first group of people to become aware of U.S. vulnerabilities, and unfortunately, they can share their knowledge with anyone.

2.6.3.1 Who is the Adversary?

Hundreds of traditional and non-traditional groups of people could be considered potential adversaries. As noted above, the cast of possibilities has been expanded in the current, multilateral environment. Anyone with a computer, modem, and telephone can access worldwide systems like the Internet from almost anywhere; and detecting and tracing such activity can be very difficult. For example, open sources report several countries are actively gathering economic intelligence data through advanced computer espionage techniques. Determining the adversary is a major part of the challenge for information warfare.

Potential opponents are interested in compromising data on various types of information systems. It has been established that the KGB sponsored the Hannover Hackers, who gained illicit access to over two dozen computer systems that contained classified information (as well as many more which did not). The Hannover Hacker case is a rare case where state-sponsored espionage has been acknowledged. DISA reporting indicates that numerous intrusions continue, and the scale of the attacks may be increasing.

Nations that are considered to be friendly to the United States have also acknowledged espionage against the United States. In almost all of these cases, the stated goal of the espionage was economic intelligence. Countries have been accused of, and have admitted to, obtaining data from the U.S. Government and U.S. corporations through information warfare-related measures. While economic intelligence may not seem to be a direct threat to U.S. security, the losses suffered by the United States are measured in billions of dollars. Additionally, any stolen technologies are no longer controlled by U.S. export regulations, and are more easily available to U.S. military adversaries. Most important, the techniques used are equally applicable to disruptive purposes. Even if not targeted against the military directly, some attacks could be mounted to disrupt significant elements of the domestic economy and infrastructure (functional attacks, as noted above), which would delay or disrupt support to the military, cause damage to the United States, and potentially cause widespread secondary effects (financial loss, cutting power or services, etc.).

Other adversaries may be concerned with transferring sensitive technologies and identifying targets for terrorist attack. This category would also include organized crime, which is concerned with the theft of funds, money laundering, extortion, etc. This category of adversary might be either a foreign or a domestic threat. There are individuals and organizations within the United States that are capable of various levels of attack. While the media has publicized the threat from individuals, there are organized groups that may be similarly disposed to harming the U.S. infrastructure. Some groups reportedly have developed units that are knowledgeable in information warfare.

From an information warfare perspective, hostile countries and terrorist organizations represent the most significant threat to U.S. national security. While economic competitors may be inclined to compromise the data on information systems, they are not likely to mount denial-of-service attacks on the infrastructure. However, economic competitors are sponsoring research that can assist hostile entities.

2.6.3.2 The Extent of the Threat

U.S. adversaries are—or certainly will be—significantly able to compromise any information system in use by the U.S. Government that has any connectivity to the outside world. Information systems, as defined for this section, would include any system involved with computing or communications.

Skilled intruders have infiltrated the foundations of PSNs throughout the world. PSNs include telephone systems and cellular communications systems. Intruders have obtained the computer software that controls the telephone systems, and there is proof that they have modified the software to include hidden ways for them to obtain access to the telephone system if authorities seal the known ways into the system. Intruders have been known to monitor conversations, reroute calls, change telephone numbers, add new telephone numbers, etc.

In view of the routing of 95 percent of military communications over commercial telephone lines, such capabilities pose a substantial threat. While the communications may be encrypted, the threat of denial of service is severe. Crippling even a small portion of the PSN could substantially impact military communications.

Commercial users of these communications networks must also be considered. Many large organizations, including the world's largest banks, rely upon public networks to perform their day-to-day operations. Billions of dollars of commerce pass over these networks every day. Intruders have been acknowledged to have compromised them. There have been several reports of criminals penetrating such communications and stealing extremely large amounts of money from financial institutions. The networks in question also provide connectivity to the U.S. Federal Reserve.

Intruders who have stolen money from financial institutions have, in some cases, been sponsored by organized crime, terrorist organizations, and hostile governments. Foreign governments are creating hacker-like capabilities. For example, friendly governments are reportedly sponsoring research on computer intrusion. While these countries might not be interested in waging information warfare against the United States, the knowledge they gain might not be confined to the friendly government.

Currently, some intruders can compromise most known countermeasures. Attackers have been able to counter dial-back modems, virus detection mechanisms, one-time password methodologies, and some encryption devices. However, technologies and procedures are available to mitigate the threat.

If technical measures are unsuccessful, intruders and other entities may resort to non-technical measures. These non-technical measures can include methods that are traditionally associated with Human Intelligence. Hackers use the term Social Engineering to describe their Human Intelligence effort. Social Engineering may include calling random people at the targeted organization and asking them for their passwords or modem telephone numbers, or going through an organization's garbage to find any information that may compromise a computer system. Generally, a Social Engineering attack may be more efficient than a traditional Human Intelligence effort, because it is more narrowly focused, and it may be easier to keep the targets unaware of such attacks.

2.6.3.3 The Unknowing Adversary

While it may appear that only a few specific entities have obtained sufficient knowledge to wage an Information War against the United States, the proliferation of the knowledge is immense. Computer criminals and hackers have developed very sophisticated methods for exchanging data. They have compromised secure computer systems on public networks, and have converted these systems so that they are used to exchange information with other hackers. The people responsible for such computer systems might never be aware of such illicit use. Computer criminals all over the world know where to go to ask for information on compromising specific types of systems. They have evolved an elaborate system of support and information sharing.

A number of the hackers are junior high, high school and college students, with the time and the ability to learn very sophisticated hacking techniques. Moreover, a growing number of intruders into computers and communications networks are not teenagers—they are professionals in the employ of others. In any case, a well connected individual can get information to compromise any type of internetted public system. There have been numerous examples of break-ins into military systems compromising sensitive data.

Many hackers do not believe they are doing anything wrong. They rationalize that they are only giving out information that should be freely available. They believe that the information should only be used for good purposes, and frown upon hackers that would try to profit from the information. While many hackers acknowledge that there are criminal crackers, they rationalize that the targeted organization should prevent people from exploiting the weaknesses that the hackers are publicizing. This mentality allows any hostile government, criminal organization, or terrorist entity to obtain the same information that is reserved for the hacker elite.

2.6.3.4 A New Source of Adversaries

Hacker knowledge may not just come from the traditional hackers. The collapse of the Soviet Union has left many extremely talented computer and communications professionals out of work and penniless. When the former Soviet Union collapsed, the funding for many technological programs was lost. Hard-working, well-meaning people were without jobs, and were forced to take jobs outside of their trained professions. These people are very easily recruited by organized crime and terrorist elements. In many cases, they are facing the same traditional enemy, except now they are being paid better.

Foreign Intelligence agents from the former Soviet Bloc are also moving to new employers. These people are extremely well trained in information warfare techniques, and can be expected to find new jobs working for U.S. adversaries. Former Soviet agents have advertised their services in a variety of publications throughout Europe.

This page intentionally left blank.

SECTION 3

ORGANIZATIONAL CONSIDERATIONS

3.1 APPROACH

Figure 3-1-1 shows the types of organizations which have an information warfare role and those which have information warfare related missions and functions.

- ***International***
- ***National***
  - **Public**
    - **Academia**
    - **Public Interest Groups**
  - **Private**
    - **Industries**
    - **Associations**
    - **Alliances**
- ***Federal Government***
  - **Executive Branch**
    - **Department of Defense**
    - **Other Departments**
    - **Interagency Groups**
    - **Advisory Committees**
  - **Independent Establishments and Government Corporations**
  - **Legislative Branch**
  - **Judicial Branch**
- ***State and Local Governments***

Figure 3-1-1. Organization Types Considered for Review

The basic approach to determining what organizational considerations might influence the development of information warfare policy and strategy included two key initial steps. The first was to identify organizations within DoD that were currently involved in information warfare activities. The second was to identify the various stakeholders in the development of the information infrastructure. The second step uncovered a very extensive and diverse set of organizations for which information warfare responsibilities are suggested, but not necessarily clearly defined. The Joint Staff Information Warfare Division (J6K) decided to focus most of the task efforts on this second set of organizations since the environmental considerations, previously addressed, appeared to be more closely related to this second set of organizations.

3.2 SCOPE

Figure 3-2-1 shows the relative number of organizations in each category (indicated by the width of the rectangles) and the relative complexity of organizational information warfare issues (indicated by the height of the rectangles). It was not possible to identify completely all of the organizations which have information warfare related missions and functions, let alone visit all the identified organizations or investigate all relevant issues. The shaded rectangles represent the coverage of differing organizations in this report.

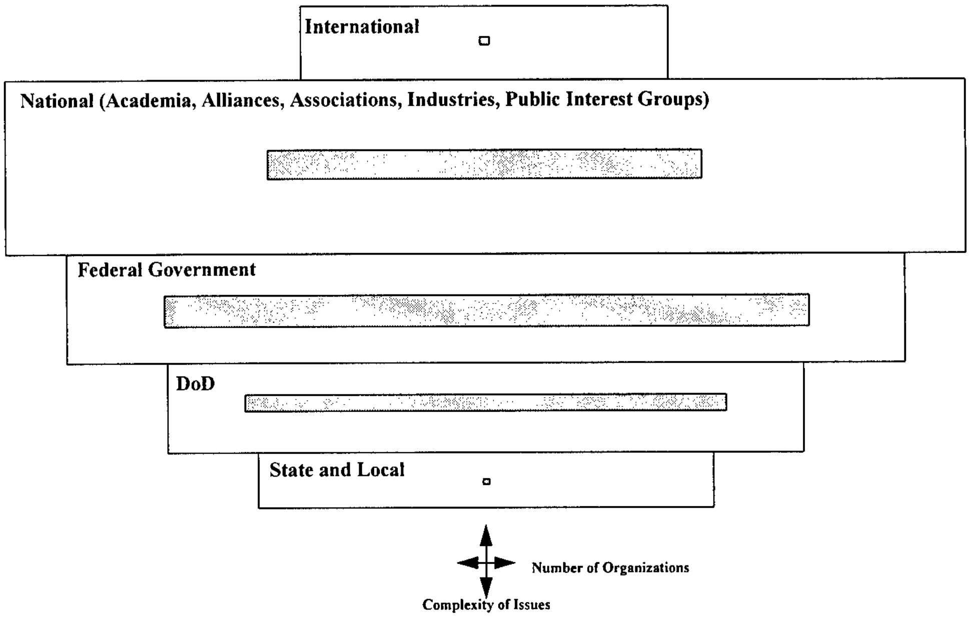


Figure 3-2-1. Scope of Organizations and Organizational Issues Addressed in Report

Because of time constraints, international and state and local organizations were not reviewed for this report. The number of these organizations and the complexity of related issues is, in fact, quite extensive. Example organizations and interests include the United Nations (coalition information warfare partners), International Telecommunications Union (international telecommunications standards, international frequency spectrum allocation), General Agreement on Trade and Tariffs (export and import controls), INTELSAT (use of international satellite communications resources), state public utilities commissions (regulation of telecommunications service providers within state boundaries) and county and city governments (regulation of cable television franchises). A review of these organizations and issues may be made in the future.

3.3 REVIEW

The review encompassed researching documents, visiting over 100 organizations, and interviewing personnel. More than half of the reviews involved visiting the organizations and interviewing key individuals in those organizations. Those organizations reviewed are identified at the index to Appendix A, Organizations and Activities. Appendix A also includes, for each organization reviewed:

- An organizational chart
- An organizational summary which identifies
  - A senior information warfare/information assurance official
  - Key points of contact
  - Information warfare/information assurance-related missions and functions
  - Information warfare/information assurance activities, issues, best practices, and lessons learned.

3.4 FINDINGS AND OBSERVATIONS

The study brought to light the following findings and observations:

- Within the Federal Government and the private sector, **there is no set of commonly agreed upon terms and definitions** to permit a meaningful discussion of what the information warfare issues are or how they might be resolved. Figure 3-4-1 illustrates some of the terms used in DoD, in other departments of the Executive Branch, and in industry. The most commonly understood terms are computer security, communications security, and information systems security.

Network Assurance **Psychological Operations** **Electronic Warfare**

Need to Know

Operations Security ***Offensive Information Warfare***

Counter C2 **Information Security** ***Confidentiality*** *Network Security*

Information-Based Warfare

Availability of Information

C2 Protect **Network Reliability** *Sensitive Unclassified Information*

Physical Destruction

Computer Security *Information Warfare - Defense* *Communications Security*

Information Technology Security

Network Integrity *Physical Security* *Command and Control Warfare*

Defensive Information Warfare *Personnel Security* *Data Integrity*

Administrative Security **Intelligence** **Information Systems Security**

Information Warfare - Offense Deception ***Classified Information***

Figure 3-4-1. Some Information Warfare Terms in Current Use

- **The DoD relies upon on a vulnerable information infrastructure that is difficult to influence.** While most of those interviewed were responsible for and familiar with COMPUSEC, COMSEC, and INFOSEC, there was a general lack of understanding of the information infrastructure vulnerabilities and, consequently, little agreement that a serious information warfare problem may exist.

- **The perception of information warfare issues is based on individual experiences and organizational missions and functions.** From the perspective of experience, the Computer Security Act of 1987 resulted in a clear division of responsibility between the DoD and the DoC regarding the protection of classified and sensitive unclassified information. The extensive and vigorous debate which preceded the legislation created a lasting impression on the participants, many of whom are now senior managers responsible for the continued implementation of the provisions of the Act. The Clipper chip proposal has solidified in the minds of industry and civil libertarians that the Federal Government must be watched at all times. And the recent establishment of the U.S. Security Policy Board has met with some resistance because some members of the Federal Government perceive that the Board may infringe on their responsibility for sensitive unclassified guidelines and standards.

  The law enforcement, defense, commerce, and intelligence communities all have significant interest in electronic intrusions and other information warfare related matters. However, because of their different missions and functions, the individual communities' perceptions of the issues may be significantly different. For example, the law enforcement community would view an electronic intrusion into a financial network as an attempt to defraud or steal and would be intent on gathering evidence to prosecute the intruder. The defense community might view it as a diversionary effort to aid in concealing a more significant intrusion into its command and control structure, as evidence of an attack on the United States, or as means to obtain funds to purchase proscribed weapons of mass destruction. The commerce community might view the intrusion as an act of economic espionage and request the assistance of the FBI, which might have competing goals vis-‡-vis the rest of the law enforcement community. And the intelligence community might view the intrusion as an opportunity to gain intelligence about the intruder. Other stakeholders have still other viewpoints.

  - Industry heavyweights, such as large telephone companies, concerned, from a competitive standpoint, in maintaining a public perception that its telephone and data networks are <u>not</u> vulnerable to disruptions.
  - Public interest groups fearful of any government involvement, which might infringe on individual rights and liberties, in the information infrastructure.
  - Professional information security associations intent on advancing the state-of-the-art in information security.
  - Government organizations concerned with the privacy of information being stored on government computers.
  - Industry associations intent on limiting government involvement in the marketplace.

  - Law enforcement organizations concerned about access to information necessary for the investigation and conviction of criminals.
  - Labor organizations concerned about preservation of jobs threatened by the efficiencies of information technology.

- **Responsibilities for information protection are not consistently assigned within the Executive Branch departments.** In some departments, all security and protection responsibilities (information, document, communications, personnel, administrative, physical, etc.) are centralized in a security organization. In other departments, the responsibilities are centralized in the Information Resources Management organization. In still other departments, the responsibilities are split among several organizational elements.

- As discussed in Section 2.1, an organizational structure and process has been created for the exchange of sensitive information related to network vulnerabilities and security in the telecommunications industry. **No other similar processes or organizations were observed during the organizational reviews,** although most individuals interviewed agreed with the need in other functional areas.

- In terms of information warfare-related capabilities, most organizations have historically focused on protection activities, and the investment strategies for the future are similarly focused. A limited number of organizations are developing capabilities to detect electronic intrusions and other disruptions. **Almost none of the organizations have developed a capability to identify the nature of the disruptions (assuming they are detected), to respond to the disruptions, or to recover from the disruptions.**

- **In many organizations, budgets and staff to address information warfare-related matters are very limited.** Staffs in the Executive Branch departments are on the order of units, tens, and scores of people. Budgets are on the order of units and tens of millions of dollars. As might be expected, everyone agrees that their budgets and staffs are much too small.

- **All organizations reviewed are faced with constant change.** Government is reinventing itself. In some cases, Executive Branch departments are being considered for elimination. In other cases, departments will be reduced in size in the next two to five years. Companies are constantly trying to adjust their work force size, form the right alliances for competitive advantage, and acquire and merge with competitors. Telecommunications legislation and regulatory reform will bring about the convergence of industries such as telecommunications, cable TV, and publishing. New technology is being introduced at an ever-increasing rate. In the face of this constant change, information security is the stepchild of operational and fiscal crises.

- **Executive-level understanding of information warfare issues is minimal but growing.** Increased press and trade publication coverage of these issues during the past year have helped to increase the level of understanding. In some departments, those responsible for information security are conducting demonstrations for senior executives on the vulnerabilities of their information and information systems.

  In spite of these seemingly discouraging words, there seems to be an extensive amount of ongoing (though uncoordinated) activity. The following are only a few of many examples:

- Within the DoD, most functional activities incorporate information warfare considerations in some fashion. These functional activities include requirements generation, research and development, acquisition, test and evaluation, intelligence, operations, training and education.

- Several organizations are conducting studies and analyses of information warfare.

- Extensive research is being initiated in the fields of information security and information warfare by the ARPA. ARPA hopes that this research will include the collaborative efforts of industry.

- Congress has directed a national cryptology policy review which may address the law enforcement and industry concerns regarding an encryption standard and the cryptology export control issues.

- At least two efforts are under way by NIST and the Information Systems Security Association (ISSA) to develop and publish generally accepted best practices for information security.

- An Interagency Group has been formed to address telecommunications and cryptology.

- An emerging variant of war games called prosperity games will enable organizations and individuals to address the economic issues related to information warfare.

SECTION 4

SUMMARY

The growing dependence of critical national security functions on a vulnerable information infrastructure poses significant challenges to the Joint Staff, the DoD, the Federal Government, and the Nation. While some activities are under way within the DoD and the Federal Government to address immediate concerns, fundamental issues must be addressed from a policy and strategy standpoint.

Those functions which are critical are not necessarily well defined as such. For those which are, the dependency on portions of the infrastructure is not well understood. However, it is certain that in times of crisis and war, demand for information to support these functions will increase significantly and the supply of information (the capacity of the infrastructure) will decrease. There has been little or no research on managing information supply and demand. The information infrastructure is an extremely complex interconnection of numerous government, public, and private networks. Much of the current dialog regarding the information infrastructure addresses the issues of security and privacy of information. There is little research regarding the functional dependencies on the infrastructure, the vulnerabilities of the infrastructure, and the means and methods to reconstitute in response to any degradation.

The evolution of the information infrastructure is influenced by a wide variety of stakeholders with very complex, diverse, competing interests. The evolution requires a balance of the needs of the state versus the rights of the individual, the Internet purists versus the market forces, privacy versus a claimed need to know, and other confrontations. Any policy initiatives seeking to influence the information infrastructure must take these stakeholders and their interests into account.

The legal environment is equally complex. Technology advances clearly outpace legal change. Legislation is generally oriented on criminal behavior and not acts of war. Given the current body of law, it is not possible to distinguish quickly between criminal acts and acts of war. And, if it were possible, there is no legislation which defines responsibilities for responding to a logical attack against the information infrastructure. The Secretary of Defense certainly has an obligation to fulfill his Title 10 responsibilities to defend the United States from acts of war, but must also honor the mandate of the Posse Commitatus Act which limits the use of the military for enforcing the law of the land. This apparent conflict must be resolved as we move toward a comprehensive national appreciation of our security needs in this area. General counsel and legislative liaison personnel well versed in the technical and operational aspects of information warfare are also needed to guide the policy makers.

The regulatory and policy environments are both noteworthy for the volume of directives and guidance. Given this volume and the laws of probability, it is nearly certain that gaps, overlaps, and conflicts exist in both regulation and policy dealing with information warfare and information assurance related issues.

The proliferation of new and emerging technologies complicates the information warfare equation. In general, the new technologies and their application reduce the costs of governing, protecting the national security, and conducting business. However, technologies such as distributed computing and open system architecture are also making the information infrastructure more vulnerable. Commercial markets alone now influence the deployment of advanced information technologies and DoD finds itself following that lead. And, the market for information technology and services is clearly international in scope, creating an equivalence in information warfare capabilities among nations, terrorist groups, ethnic groups, and individuals.

This proliferation of technology and equivalence of potential adversaries poses significant challenges for the intelligence community. For example, what are the indicators of an information warfare attack? How can the United States detect an information warfare attack and distinguish it from a crime, mistake, or accident? If an attack is detected, how can the United States trace the origins of the attack and identify the attacker? The proliferation of technology also raises significantly the possibility of denial of service attacks against the information infrastructure. If we are reluctant to exercise degraded communications during war games and exercises, we must now consider the real possibility of no updated information in the conduct of war.

Finally, it is becoming evident that a very broad skill set is required to address these information warfare and information assurance policy and strategy issues. Operational, doctrinal, systems, networks, infrastructure, technology, political, diplomatic, business, and legal skills are only a few of the skills needed to address these complex issues. In this dawning information age, we have the technical capability to quickly assemble and apply these diverse skills to the issues.

Many of our nation's political and military leaders are deeply concerned about the dependency of key national security functions on a vulnerable information infrastructure. This issue is one of extreme complexity and one which will not be resolved in one or two years. It will require extensive discussion involving representatives from many differing points of view—political, diplomatic, economic, military, commercial, and technical, to name a few. This report was commissioned to help the Joint Staff better prepare to participate in and contribute to these discussions. The report is offered for the same purpose to the larger community to aid in addressing this national security issue of growing urgency and importance.

APPENDIX A
TABLE OF CONTENTS

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Organization Page

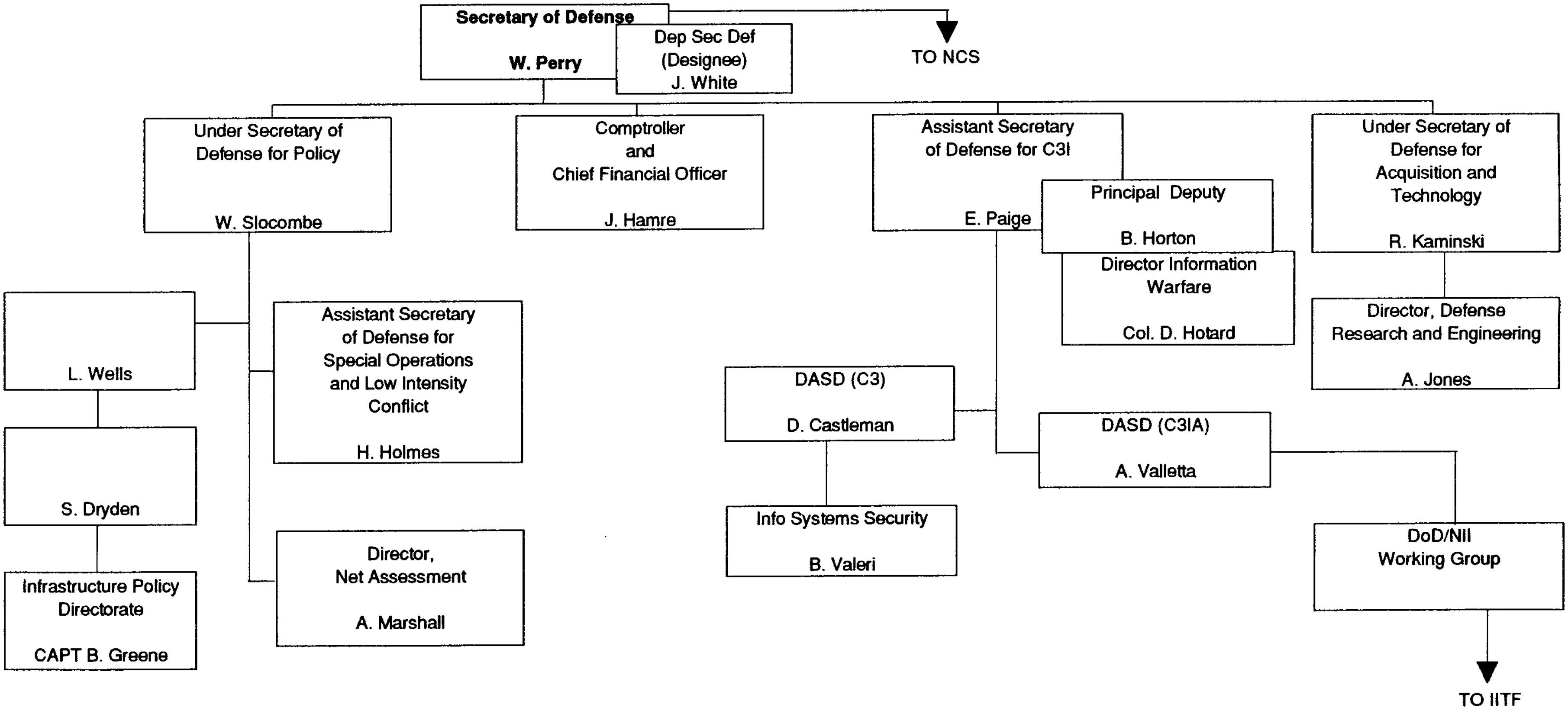
Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

This page intentionally left blank.

Department of Defense



Secretary of Defense
W. Perry

Dep Sec Def
(Designee)
J. White

TO NCS

Under Secretary of Defense for Policy
W. Slocombe

Comptroller and Chief Financial Officer
J. Hamre

Assistant Secretary of Defense for C3I
E. Paige

Principal Deputy
B. Horton

Director Information Warfare
Col. D. Hotard

Under Secretary of Defense for Acquisition and Technology
R. Kaminski

Director, Defense Research and Engineering
A. Jones

L. Wells

S. Dryden

Infrastructure Policy Directorate
CAPT B. Greene

Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
H. Holmes

Director, Net Assessment
A. Marshall

DASD (C3)
D. Castleman

Info Systems Security
B. Valeri

DASD (C3IA)
A. Valletta

DoD/NII
Working Group

TO IITF

Organization: Office of the Assistant Secretary of Defense (C3I)

Senior Information Assurance Official:

Emmett Paige, Assistant Secretary of Defense (C3I)

Information Assurance Points of Contact:

Barbara Valeri, Director, Information Security
Colonel Doug Hotard, Director, Information Warfare

Information Assurance Related Missions and Functions:

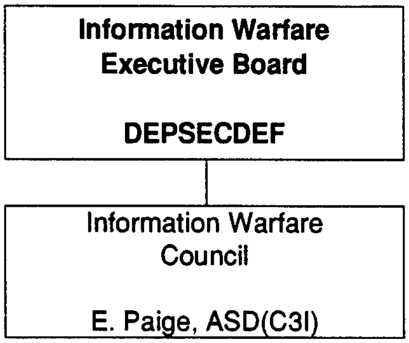
The ASD(C3I) has established a Directorate for Information Warfare reporting directly to the Principal Deputy to help the ASD(C3I) execute his task as the senior Information Warfare advisor to the Secretary of Defense and senior policy official in the Department for Information Warfare.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OMB has an Information Security Oversight Organization headed by Steve Garfinkel which was created under the provisions of Executive Order (E.O.) 12356, National Security Information.
- Expect revision to E.O. 12356 to be signed soon. Revision is expected to radically alter the information which must be protected, etc. Looking for any mention of U.S. Security Policy Board in the revised E.O.
- Information Systems and Classification Management Working Groups of Security Policy Forum are still not off the ground because of civil agency concern about "national security related information."
- Current version of the Paperwork Reduction Act exempts DoD and intelligence activities from certain provisions for OMB oversight. Revision to Act may not provide these exemptions.
- Vulnerability of nation to information disasters is generally accepted. It is not clear what the responsibilities should be for dealing with the issues.
- The ASD(C3I) is supporting the National Security Council in drafting a Presidential Review Directive on Information Assurance for their consideration and action.
- The ASD(C3I) has requested an Intelligence Community Assessment and National Intelligence Estimate of the foreign Information Warfare threat with emphasis on the physical threat to the infrastructure supporting the Public Switched Network and the electronic threat to the information present on and accessible through the network.
- The ASD(C3I) sponsored an executive forum in January, 1995, to discuss critical Information Warfare issues facing the DoD.

- The ASD(C3I) is revising the current DoD Directive 3600.1 to reduce the classification and, thereby, increase knowledge and awareness of the Department's policy and responsibilities for IW.
- The ASD(C3I) is investigating and will support an active "Red Team" effort with the USD (A&T).
- The ASD(C3I) has developed and is coordinating a formal "Defensive Information Warfare Strategy."
- The ASD(C3I) and the President, National Defense University are exploring ways for the NDU to assume a central role in Information Warfare education and awareness.
- The USD(P) Office of Net Assessment and the ASD(C3I) have initiated a "Net Assessment of Information Warfare" as suggested by the Defense Science Board's 1994 Summer Study.
- The new Defense Planning Guidance (DPG) contains specific reference to enhanced Defensive Information Warfare/Information Assurance programs.
- The Deputy Secretary has established and will chair an Information Warfare Executive Board across the Department. The ASD(C3I) will chair the supporting Information Warfare Council.
- The Deputy Secretary sponsored a "Day After ..." game for members of his Executive Board and has invited members of the NSTAC Industry Executive Subcommittee to participate.
- The Deputy Secretary's IW Executive Board and ASD(C3I)'s Council will sponsor additional seminars, topical forums, and other events to bring the Department together with interested parties outside the Department to address critical IA issues.

This page intentionally left blank.


Information Warfare Executive Board
DEPSECDEF
Information Warfare Council
E. Paige, ASD(C3I)

Organization: Information Warfare Executive Board (IWEB)

Senior Information Assurance Official:

Deputy Secretary of Defense, Chairman

Information Assurance Points of Contact:

Emmett Paige, Assistant Secretary of Defense (C3I)
Colonel Doug Hotand, Director, Information Warfare, OASD(C3I)

Information Assurance Related Missions and Functions:

The IWEB is a DoD working group, established by the DEPSECDEF, to address IW planning, policy, and legal issues. The Board will be chaired by the Deputy Secretary of Defense. Membership will include the Vice Chairman, Joint Chiefs of Staff, the DDCI, Director, NSA, Director DIA, USD(P), USD(A&T), Comptroller, General Counsel, Director DISA, NSC representative, and ASD(C3I). The IW Executive Board will have a supporting IW Council, composed of deputies, which will supervise supporting work for the Board. Secretariat support is provided by OASD(C3I). Other representatives from the Federal government may be invited.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Board will be briefed on IW issues, participate in wargames which incorporate IW activities, is expected to address IW roles and responsibilities, and will serve as the DoD focal point for IW discussion at the National level.

Organization: Infrastructure Policy Directorate, Office of the Under Secretary of Defense (Policy)

Senior Information Assurance Official:

Mr. Linton Wells, Deputy to the Under Secretary of Defense (Policy) for Policy Support

Information Assurance Points of Contact:

Ms. Sheila Dryden, Director, Emergency Preparedness Policy
CAPT Brent Greene, Director, Infrastructure Policy Directorate

Information Assurance Related Missions and Functions:

The Infrastructure Policy Directorate is responsible for shaping policy issues pertaining to DoD infrastructure and future directions for information protection, including interagency and interdepartmental coordination.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Developed extensive "out-of-box" methodology for identifying dependencies within various infrastructures, critical nodes in the infrastructures, and dependencies among several infrastructures. Methodology includes modeling and simulation of industries and of the synergy between industries and infrastructures. Categories of infrastructures include:
    - Military - forces, facilities, command and control
    - Traditional infrastructures - water and sewage, electrical power, telecommunications, transportation, petroleum, oil, and lubricants, space
    - Industries - weapons, heavy machinery, steel, electronics/computers
    - Commodities - coal, foodstuff, chemicals, raw materials, irreplaceable components
    - Political, economic, and social - environment, crime/security, health/safety, society, culture, economy/finance, political leadership, diplomacy
- Look at vulnerabilities of Supervisory Control and Data Acquisition (SCADA) networks.
- Need to add network and modeling and simulation expertise to our intelligence estimates.
- Concerned about how to insert infrastructure thinking into the Department of Defense processes - Defense Planning Guidance, Contingency Planning Guidance, National Military Strategy, National Security Strategy.
- Shaping the role of DoD in the protection of infrastructures, including coordination between DoD and non-DoD government, and civilian/corporate owned/operated infrastructures.

Organization: Office of Net Assessment (OSD/NA)

Senior Information Warfare Official:

Director, OSD/NA, Mr. Andrew W. Marshall

Information Warfare Points of Contact:

COL Chuck Miller, USAF, Military Assistant
CAPT Jim FitzSimonds, USN, Military Assistant
CDR Jan van Tol, USN, Military Assistant

Information Warfare Related Missions and Functions:

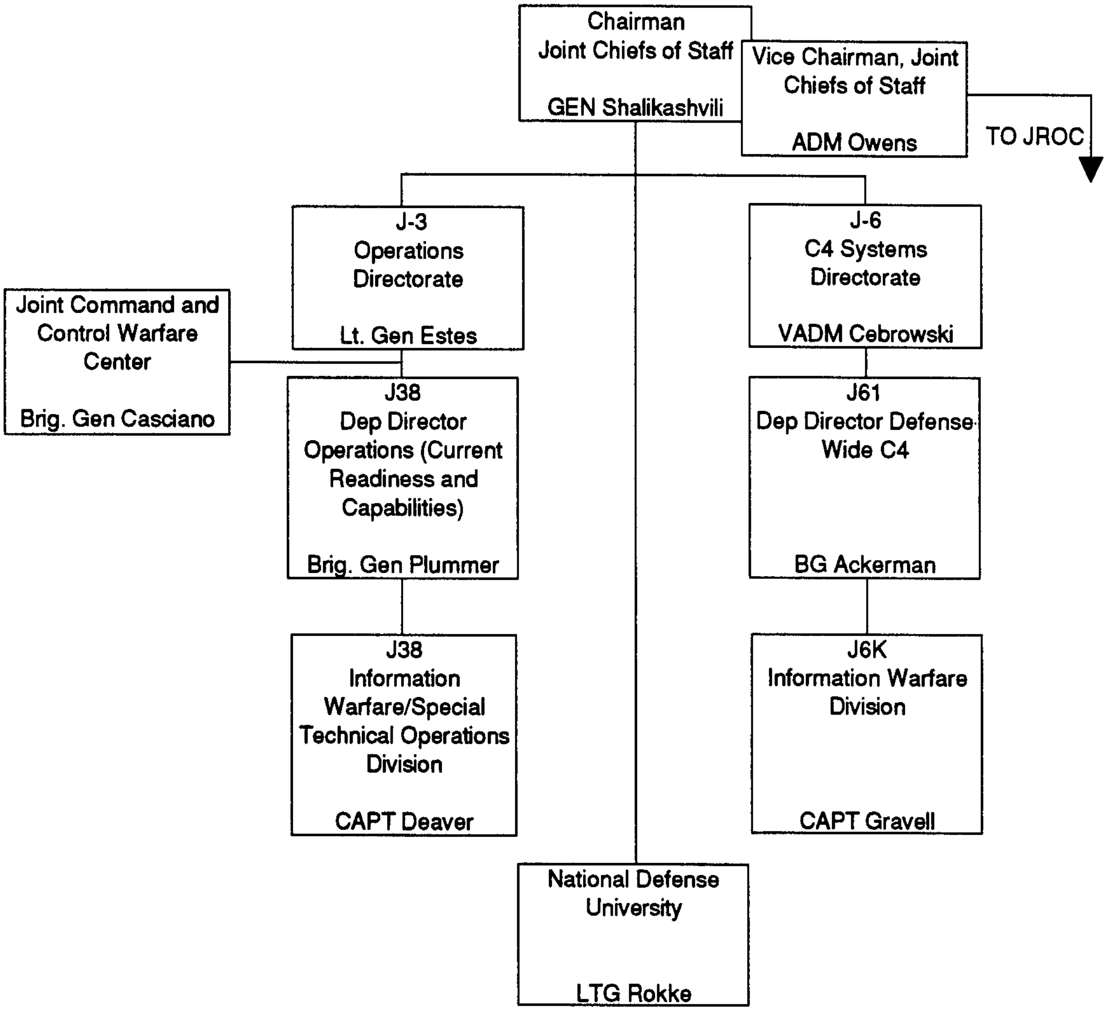
The Director of OSD/NA provides long-term analytic support to the Secretary of Defense and, when the SECDEF directs, to other senior officials in the Department (USD(P), USD (Acquisition), the Chairman, JCS, and the CINCs), on issues and trends in military affairs of potential import for the Department. Much of the analytic work of the office is engaged in preparing net assessments of the military balances in regions or in functional areas. The Director also makes recommendations regarding the DoD studies and analyses which are contracted outside the department. Information warfare was identified as a potentially important new warfare area several years ago in OSD/NA, and has been the subject of a widely ranging study effort ever since, within the office, and via contract, outside the office and with each of the Services and JCS.

The Defense Science Board Summer (1994) Study on Information Architecture for the Battlefield recommended a Net Assessment to be done in the Department on IW. Their assessment was begun earlier this year. OSD/NA has set up advisory panels of key people from within the military and JCS to advise as this work is executed. Colonel Miller is currently the POC in OSD/NA for the Assessment.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- In addition to the Net Assessment, there is a long-term study effort under way which involves a series of workshops, seminars (IW Infrastructure, MOEs, Gaming and Simulation, Training, Intelligence, etc.), and wargames (Dec., 93, Oct., 94), as well as efforts with ASD/C3I and the Intelligence Community to explore the dimensions of IW, policy and strategy issues for the Department, and the policy issues relating to agencies beyond DoD of importance for the Department.

THE JOINT STAFF


Chairman
Joint Chiefs of Staff
GEN Shalikashvili
Vice Chairman, Joint Chiefs of Staff
ADM Owens
TO JROC
J-3
Operations Directorate
Lt. Gen Estes
J-6
C4 Systems Directorate
VADM Cebrowski
Joint Command and Control Warfare Center
Brig. Gen Casciano
J38
Dep Director Operations (Current Readiness and Capabilities)
Brig. Gen Plummer
J61
Dep Director Defense-Wide C4
BG Ackerman
J38
Information Warfare/Special Technical Operations Division
CAPT Deaver
J6K
Information Warfare Division
CAPT Gravell
National Defense University
LTG Rokke

Organization: The Joint Staff

Senior Information Warfare Official:

LtGen Howell M. Estes III, J3
VADM Arthur K. Cebrowski, J6

Information Warfare Points of Contact:

CAPT William Gravell, Division Chief, Information Warfare Division, J6K
CAPT William N. Deaver, Jr., Division Chief, Information Warfare/Special Technical Operations Division, J38

Information Warfare Related Missions and Functions:

J38 IW-STOD is responsible for all offensive information warfare programs and activities coordinated by the Joint Staff. J6K is responsible for all defensive information warfare programs and activities coordinated by the Joint Staff. The two divisions fully share responsibility for all aspects of broad policy, assessment and doctrine. A Memorandum of Understanding between the two organizations and frequent collaboration on information warfare activities ensures fully coordinated actions.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Ongoing training and education initiatives include implementing information warfare in exercises, coordinating Service training initiatives under the auspices of the Inter-Service Training Review Organization, and the development of an education strategy to infuse information warfare into the broad defense academic community.
- Policies and security classification guidance for information warfare are currently being developed.
- Command and Control Warfare doctrine is currently being coordinated. Information protection doctrine is being developed and incorporated in various doctrinal efforts.
- The Joint Warfighter Capability Assessment (JWCA) process includes studies of information warfare offensive and defensive capabilities, emerging technologies, and intelligence support to IW. Additionally, the JWCA includes an effort to examine Service and Agency Program Objective Memorandum submissions relative to the Defense Planning Guidance and CINC requirements.
- J6K is studying nascent technologies outside of the requirements process to determine if some may have information warfare applications.
- J6K is leading an effort to develop a requirement for rigorous modeling and simulation capabilities that would contribute to a comprehensive national information warfare defense.
- J6K is reexamining multi-level security (MLS) concepts and requirements and incorporating these concepts into information protection architecture efforts. J6K is working with the CINCs to define new MLS requirements and refine existing MLS requirements, and is establishing development and fielding priorities.

Organization: School of Information Warfare and Strategy (SIWS), Information Resources Management College (IRMC), National Defense University (NDU)

Senior Information Warfare Official:

LTG Rokke, President, NDU
Dr. John Alger, Director, School of Information Warfare and Strategy (SIWS)

Information Warfare Points of Contact:

Dr. Fred Giessler, Professor, SIWS, and Information-Based Warfare Course Manager
CDR Earle L. Rudolph, Jr., Professor, SIWS
Mr. Bradley E. Barriteau, Professor, SIWS
Mr. Tom Czerwinski, Professor, SIWS
Dr. Dan Kuehl, Professor, SIWS

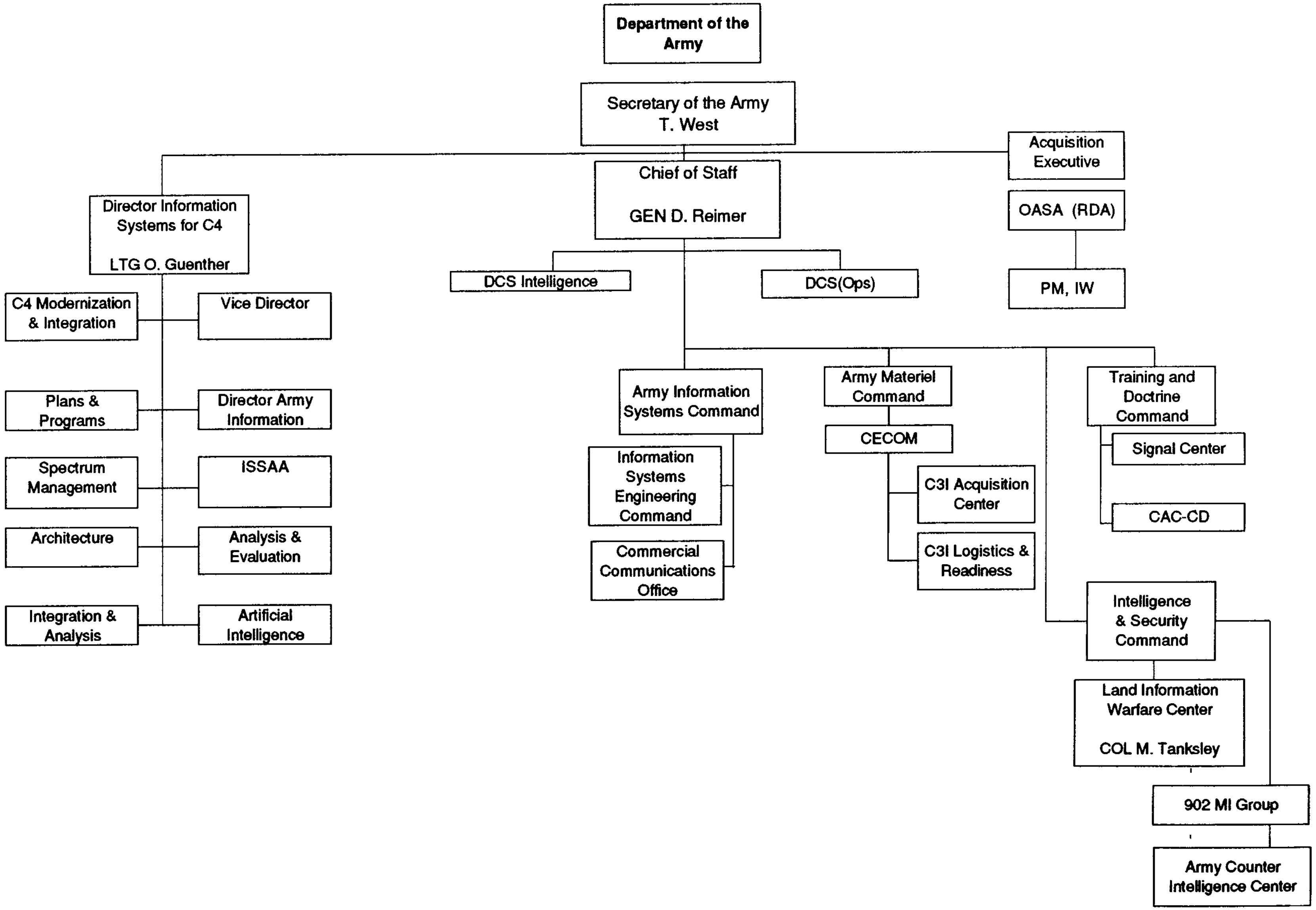
Information Warfare Related Missions and Functions:

The School of Information Warfare and Strategy completed on June 14, 1995, the first year of a 2-year senior-level joint program, has become a fully equivalent, one-year alternative to the National War College and Industrial College of the Armed Forces at NDU. The first full-year program was started in August 1994, with a pilot class of 16 students representing the same joint origins and senior level as the other two colleges. The course is a level one PME equivalent, oriented towards Information Warfare and all of its implications for national power and joint warfare. The College also teaches quarterly a one week, intensive course on Information-Based Warfare to students from every service and the military and civilian agencies. The one-week course focuses on introducing the evolving concepts of information warfare, describing its principles and elements, and investigating current initiatives relating to joint operations, and national and international security objectives. The IRMC provides a forum for joint consideration and research into Information Warfare as a concept, and integrating the principles into joint warfare planning and operations.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The expanded IRMC Information Warfare curriculum remains a small part of the larger NDU community. IRMC also teaches a number of related courses which focus more heavily on the technical component of information management technologies. The full year course will enter its second year in Fall 1995, and continues to evolve. The short, one-week program is consistently oversubscribed, and provides a quick introduction to the IW idea and its current implications. The school provides a focal point for consideration and elaboration of some of the joint issues for the military. It has also served as a forum for other related IW activities, e.g., games and the like.

This page intentionally left blank.


Department of the Army
Secretary of the Army T. West
Chief of Staff GEN D. Reimer
Acquisition Executive
OASA (RDA)
PM, IW
Director Information Systems for C4 LTG O. Guenther
DCS Intelligence
DCS(Ops)
C4 Modernization & Integration
Vice Director
Plans & Programs
Director Army Information
Spectrum Management
ISSAA
Architecture
Analysis & Evaluation
Integration & Analysis
Artificial Intelligence
Army Information Systems Command
Information Systems Engineering Command
Commercial Communications Office
Army Materiel Command
CECOM
C3I Acquisition Center
C3I Logistics & Readiness
Training and Doctrine Command
Signal Center
CAC-CD
Intelligence & Security Command
Land Information Warfare Center COL M. Tanksley
902 MI Group
Army Counter Intelligence Center

Organization: Department of the Army

Senior Information Warfare Official:

Chief of Staff of the Army

Information Warfare Points of Contact:

GEN Tolelli, Vice Chief of Staff of the Army
Dr. Herb Fallen, Assistant Secretary of the Army for Research, Development, and Acquisition
LTG Paul E. Blackwell, DCSOPS
MG Scales, Deputy DCSOPS for Operations and Plans
MG Anderson, Deputy DCSOPS for Force Development
MG Oder, Vice Deputy DCSOPS for Force Development
MG Paul E. Menoher, Acting DCSINT
Mr. David E. Borland, Acting ODISC4
MG Boyd, Chief of Doctrine (TRADOC)
BG Trent N. Thomas, INSCOM
COL Mike Tanksley, Commander, Land Information Warfare Activity
LTC Irons, Commander, Army IW Office Studies & Analysis Activity
LTC Schmidt, Commander, Army IW Office Concept & Doctrine Office
LTC Kelly, Program Manager for Army Information Warfare
Phillip Loranger, Army Information Security Management Office (ISMO)

Information Warfare Related Missions and Functions:

ISMO is subordinate to ODISC4. The mission of ISMO is to secure Army AISs. One of the key tasks assigned to this office by letter directive from ODCSOPS is the development of a Defensive Information Warfare Program Management Plan. (There are 4 pillars to the proposed plan: Policy, Organization, Equipment, and Training.) Development of the PMP is in its infancy. ISMO is also rewriting AR 380-19.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- General Comments: At the Army Staff level, there are 4 elements performing Information Warfare activities: Assistant Secretary of the Army (Research/Development/Acquisition) (SARDA), ODCSOPS, ODCSINT, and ODISC4. (The Army JAG also has involvement.) General Rigby heads the Army Digitization Office and is responsible for the Force XXI project, and has an interest in Information Warfare.
- At the Army major command level, the following organizations are involved in one way or another with Information Warfare: INSCOM, Ft. Belvoir, VA; ISC, Ft. Huachuca, AZ; TRADOC, Ft. Monroe, VA; and the Army supported CINCs. Elements within

TRADOC are: Combined Arms Center, Ft. Leavenworth, KS; Centers and Schools (Intelligence Center/School, Ft. Huachuca, and Signal Center/School, Ft. Gordon, GA); and the Army War College, Carlisle Barracks, PA.

- Other Army elements involved with Information Warfare include the Land Information Warfare Activity (LIWA), Ft. Belvoir; Psychological Operations Command; and, Special Operations Command.
- ISMO views its Information Warfare responsibilities, where an active response is required, as distinct from INFOSEC, which involves only passive response. In their view, INFOSEC loosely encompasses the traditional terms, COMSEC and COMPUSEC.
- The Army is attempting to orchestrate a unified approach to Information Warfare that encompasses:
  - Training for system/network administrators.
  - An organizational structure to exchange critical information (example: Directors of Information Management were formerly centralized under Information Systems Command (ISC), but with DMRD 918 they reverted to the major commands; additionally DMRD 918 forced a great deal of consolidation, e.g., the Network Management Center at 7th Signal, but the Army later lost 7th Signal Command).
  - Automated tools to support System Administrators -- "the Army's DIW Warrior." A key Army requirement is automated detection tools.
- The challenge for the Army, like other Services and agencies, is to balance security needs and investments with other critical warfighting requirements.

Organization: Army Information Warfare Office, Department of the Army, Falls Church, VA

Senior Information Assurance Official:

COL John Holland, Commander, Army Information Warfare Office

Information Assurance Points of Contact:

MAJ Bob Evans
MAJ Joann Webber
Mr. William M. McDowell

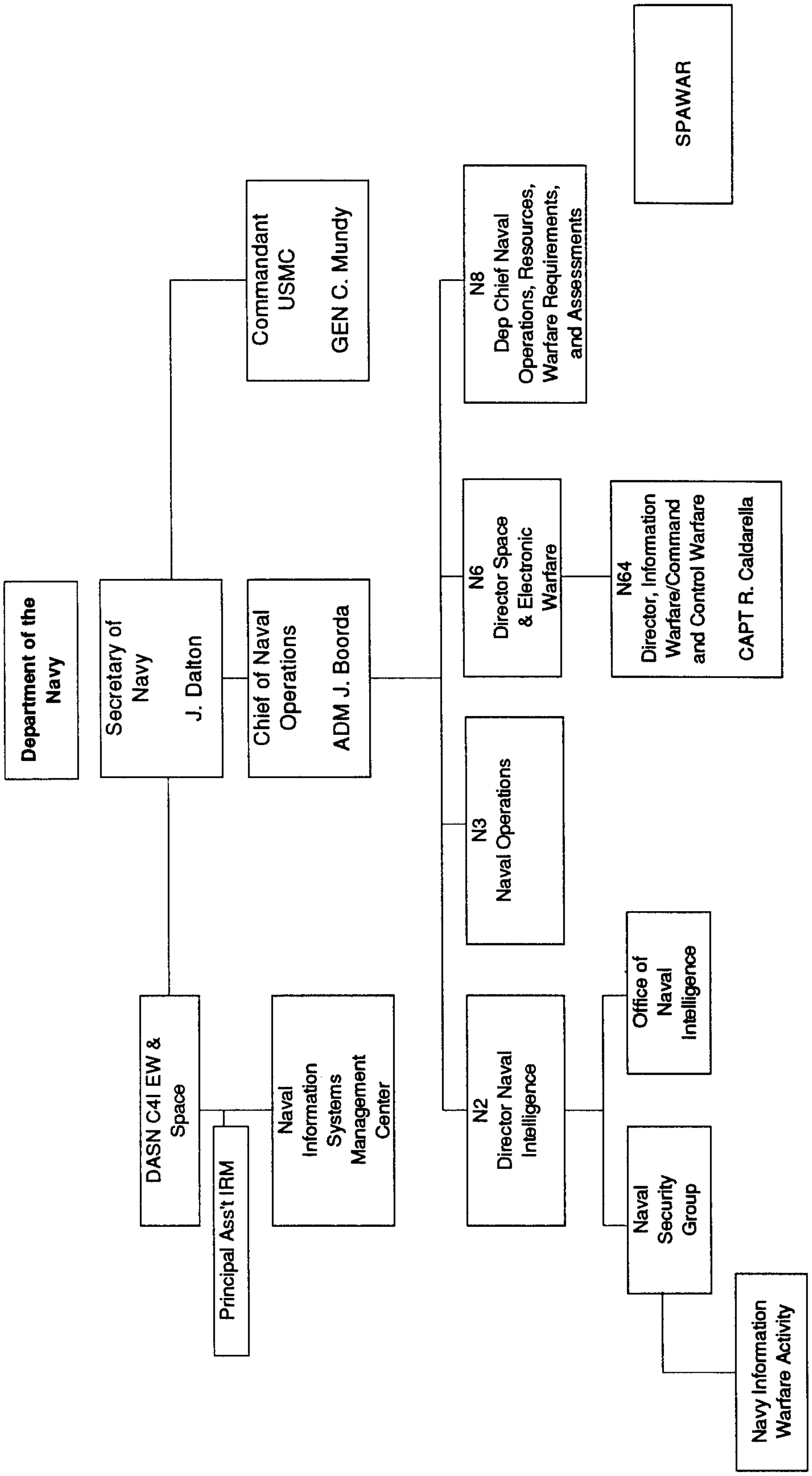
Information Assurance Related Missions and Functions:

Following Desert Storm, it was apparent to the Army that information warfare required increased emphasis. The Army Modernization Plan (Spring 1992) captured the concept, "Win the Information War." Numerous activities have taken place in the Army since that time. A C2- Protect Council of Colonels was created in 1993 to deal with the protection of C2 assets essential to the success of information warfare. In 1994, the Land Information Warfare Activity (LIWA) was formed to focus on operational support to military forces. The Army IW Office was also formed to deal with force modernization issues. Many studies, master plans, and symposia have been held to push the Army closer to a Force XXI capable of winning the IW war. Drafting of doctrine by TRADOC has received renewed emphasis. The Army generally refers to information operations rather than information warfare.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Information Warfare, per se, is not limited to DoD in the Army's view. Conversely, C2W is limited to the military. As with other services, Army views the legal aspects of IW, particularly during "Operations Other Than War" to be a large issue. Within the legal realm, initiatives involving technology such as embedding the capability to disrupt functionality must be viewed carefully if IW objectives are envisioned.
- For self protection, should we build systems with unique signatures or systems which appear like all others to add to the computer security posture?
- Army sees the need for migration to capabilities-based assessments vs. threat-based assessments. Capabilities in this sense can be interpreted as technology.
- Army is conducting three studies involving IW. One is classified. A second is being performed by LIWA and is targeted toward validating existing requirements and generating additional requirements. TRADOC is conducting a third study on EW capabilities.
- Concepts:
  - * Information Warfare Attack Capability (IWAC).
  - * Assets include INSCOM, AFCSC, and NSG. ODISC4 is responsible for DIW. DISC4 and the Council of Colonels (chaired by COL Holland) are examining risk management. From a C2 protect standpoint, we can't afford to fix today's force. That must be done with procedures. What we can afford must be allocated by prioritization; risk management must be performed on the rest. We must embed IW in Force 21 through protection programs in the acquisition system. Today's acquisition cycle is not responsive to threats and vulnerabilities. Technology is moving too fast. Army has pursued appliqués as an interim approach to beating the technology cycle.
  - * OIW data and DIW data must be exchanged.
  - * A challenge for the Army in IW is acquiring policy direction from above.
  - * Information Operations encompasses IW, which encompasses C2 Warfare.

This page intentionally left blank.


Department of the Navy
Secretary of Navy
J. Dalton
Commandant USMC
GEN C. Mundy
Chief of Naval Operations
ADM J. Boorda
DASN C4I EW & Space
Principal Ass't IRM
Naval Information Systems Management Center
N2
Director Naval Intelligence
Office of Naval Intelligence
Naval Security Group
Navy Information Warfare Activity
N3
Naval Operations
N6
Director Space & Electronic Warfare
N64
Director, Information Warfare/Command and Control Warfare
CAPT R. Caldarella
N8
Dep Chief Naval Operations, Resources, Warfare Requirements, and Assessments
SPAWAR

Organization: Department of the Navy

Senior Information Warfare Official:

VADM W. J. Davis, Director, Space and Electronic Warfare

Information Warfare Points of Contact:

LCDR Gary Burnette, Chief of Naval Operations (OPNAV) (N64)
CAPT Rocco Caldarella

Information Warfare Related Missions and Functions:

Internal Roles and Responsibilities: N64 is responsible for the development of requirements, plans, and program development of IW in the Navy. The office is the de facto day-to-day point of contact for all IW matters in the Navy.

Interagency Activities: The Navy subscribes to the direction provided in DoD Instruction TS3600.1 and MOP 30. IW is implemented operationally at the direction of the National Command Authority, through the Unified CINCs to the Fleet CINCs and Marine Corps, and down to Task Force and Groups with IW-capable units. From an administrative perspective, CNO implements IW through N6 as described above, and N3 for Policy Development.

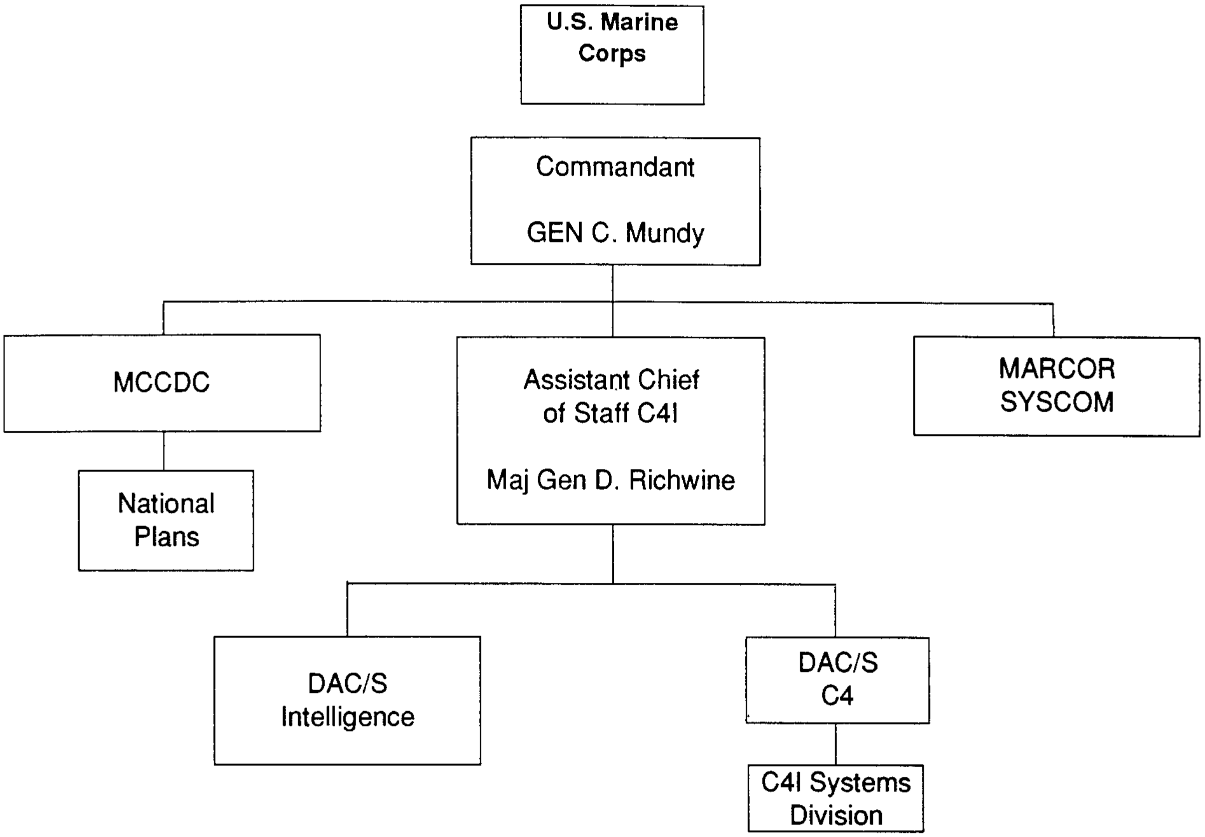
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- CNO has issued several recent instructions, most notably OPNAVINST 3430.25, of April 1994, which established Navy IW policy, and OPNAVINST 3430.26, of 17 January 1995, Implementation Instruction for Information Warfare/Command and Control Warfare (IW/C2W). Doctrine is being written by the Naval Doctrine Command; a copy of NDP-6 is in draft. COMNAVSECGRU has been designated as the Executive Agent for Information Warfare for N6. CNO directed a Personal For to the Fleet CINCs last year and stressed how serious he was about IW. Currently pending are IW Policy Guidance, and a Mission and Functions Statement for the FIWC and the NIWA.
- CNO's IW strategy is focused around the following concepts: Embedded in the Force; Forward Presence (ships, planes, SEALS, USMC, and recce assets); Agile Acquisition Strategy; and the cryptologic capabilities of the Naval Security Group.
- Visible activities which reflect promotion of IW in the Navy include:
  - * The establishment of the Naval Information Warfare Activity (NIWA), now at 3801 Nebraska Avenue, but to be moved to Fort Meade this year (along with the rest of NSG).
  - * The pending establishment of FIWC at Little Creek, VA with a detachment in San Diego, CA. This center would be formed from existing Fleet Deception Group/C2W Group assets, and would support the Fleet CINCs.

- * The Chief, Naval Education and Training (CNET) created a Tiger Team which has evaluated entry level training requirements for Information Warfare. IW/C2W is now being taught at OCS, Surface Warfare Officer School, and at Boot Camp.
- * An IW career pipeline is being established and has been supported by CNO.

- The Navy staff is promoting capitalizing on existing resources to the maximum extent possible. Implementation of IW is going to be an evolutionary process.
- Acquisition is a major problem in developing the POM to support IW given the turnover in technology being so short. Not only are there difficulties in designating which specific items to buy (in FY98/99/00), but which color of money in which to allocate spending.
- There needs to be a unifying set of standards/IW common core functions. CNO has identified the following items as fitting into those categories: Policy, Definitions, Data Bases, Modeling/Simulation Standards, Mission Planning, Training, Agile Acquisition, C4I, SOPs.
- A national IW policy is critical to any success in DoD and the Navy.
- Roles and missions of the Services must be defined.

This page intentionally left blank.


U.S. Marine Corps
Commandant
GEN C. Mundy
MCCDC
National Plans
Assistant Chief of Staff C4I
Maj Gen D. Richwine
MARCOR SYSCOM
DAC/S Intelligence
DAC/S C4
C4I Systems Division

Organization: United States Marine Corps

Senior Information Warfare Official:

Lieutenant General A. C. Blades, Deputy Chief of Staff for Policy, Plans, and Operations

Information Warfare Points of Contact and Areas of Interest:

Major Bob Wiedower (Code PLN: National Plans)
Colonel Bouldry (INFOSEC/COMPUSEC)
Lieutenant Colonel Robb (SIGINT)

Information Warfare Related Missions and Functions:

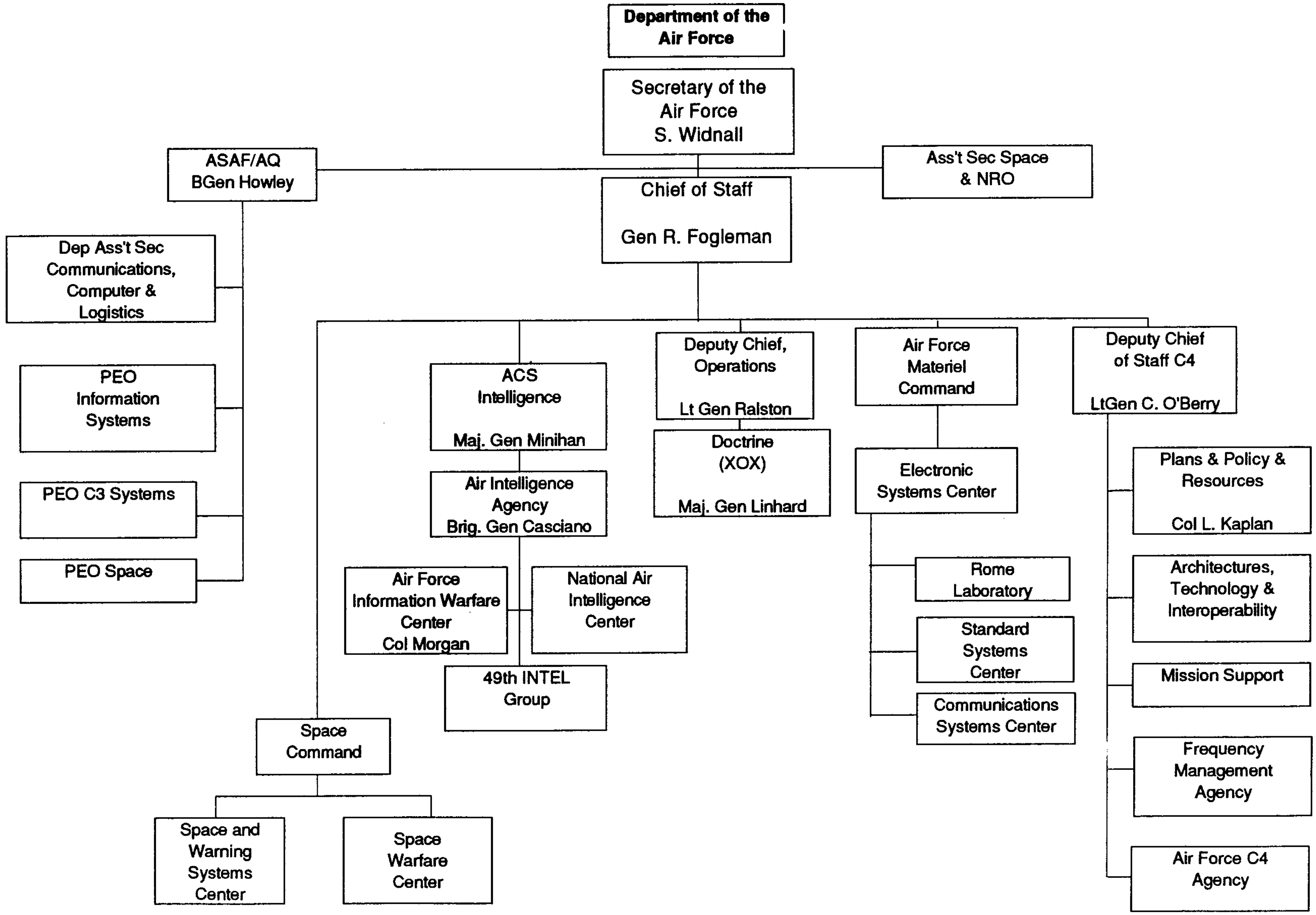
Within the Plans, Policy, and Operations Department at HQMC is the National Plans Branch which has direct responsibility for Information Warfare policy. Others within the HQ who have an interest in IW are the C4I Department, within which are responsibilities for INFOSEC and COMPUSEC, and Computers, Intelligence, and SIGINT.

HQMC has established an IW working group to coordinate IW activities between all HQMC departments, the Marine Corps Combat Development Command (MCCDC), and the operating forces.

There is one document pertinent to Marine Corps IW -- Marine Corps Order 3430.5A, Policy for Command and Control Warfare (C2W). The Marine Corps is currently developing doctrine for C2W.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The lack of a national policy is inhibiting agency-wide coordinated planning.
- The Marine Corps is investigating ways to ensure C2W tools get down to the operating forces.
- The Marine Corps is fully participating in Joint IW training efforts.


Department of the Air Force
Secretary of the Air Force S. Widnall
ASAF/AQ BGen Howley
Ass't Sec Space & NRO
Chief of Staff Gen R. Fogleman
Dep Ass't Sec Communications, Computer & Logistics
PEO Information Systems
PEO C3 Systems
PEO Space
ACS Intelligence Maj. Gen Minihan
Air Intelligence Agency Brig. Gen Casciano
Air Force Information Warfare Center Col Morgan
National Air Intelligence Center
49th INTEL Group
Deputy Chief, Operations Lt Gen Ralston
Doctrine (XOX) Maj. Gen Linhard
Air Force Materiel Command
Electronic Systems Center
Rome Laboratory
Standard Systems Center
Communications Systems Center
Deputy Chief of Staff C4 LtGen C. O'Berry
Plans & Policy & Resources Col L. Kaplan
Architectures, Technology & Interoperability
Mission Support
Frequency Management Agency
Air Force C4 Agency
Space Command
Space and Warning Systems Center
Space Warfare Center

Organization: Department of the Air Force

Senior Information Warfare Official:

Information Warfare Points of Contact:

LtCol Ray Michael USAF, Air Staff, Assistant Chief of Staff, Intelligence
COL Gregg Wheeler
LtCol Ernest Zernial

Information Warfare Related Missions and Functions:

Internal Roles and Responsibilities: The Assistant Chief of Staff, Intelligence (ACSI) has taken the lead in coordinating doctrine for Information Warfare in the Air Force. ACSI is addressing doctrine and policy issues, and integrating Information Warfare into the Air Force with the concurrence and cooperation of the Deputy Chief of Staff for Ops (XO) and the Assistant Chief of Staff for C4 (SC). It is anticipated that once IW is more firmly defined and established, that XO (primarily for Ops/Offensive IW implementation) and SC (primarily for DIW) will assume greater roles.

Interagency Activities: The relationships and activities of the key IW organizations can be found on the organization chart. CSAF directed the ACSI and the Deputy Chief of Staff for Operations to staff an approach to IW for the Air Force to establish doctrine and policy with Air Force major commands, and then the CINCs.

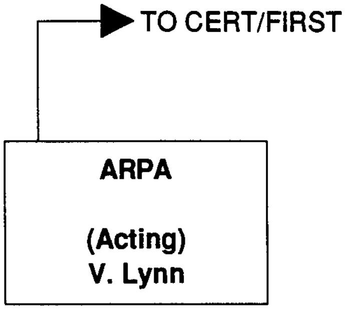
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- As with the other services, Air Force is following the lead established by DoD Directive TS3600.1, MOP 30, and (draft) JCS Pub 3-13. As doctrine is being developed for the Air Force, three objectives have been identified:
  - Control the information realm so that we can exploit it while protecting our information operations from enemy action. That is, use information, but deny it to the enemy; emphasize superior access to information.
  - Exploit control of information to employ information warfare against the enemy.
  - Enhance overall force effectiveness by fully developing information operations.
- Translating these objectives into the roles of air power, we have: Control, Employ, Enhance, and Support. The Air Force has also chosen to use these subdivisions as a decomposition, which corresponds to their implementation of Information Warfare. The key point here is that Information Warfare is viewed as embedded in the roles of air power, and the two disciplines cannot be separated.
- Control has three subsets: Counterair, Counterspace, and a new concept called Counter Information, which itself has components of Offensive Counter Information and

Defensive Counter Information. Offensive Counter Information consists of Enable/Exploit (Physical Attack, Deception, PSYOP, EW, and Special Technical Ops), and Disable/Protect (Physical Attack, EW, Special Technical Ops, and Public Affairs). Defensive Counter Information consists of Active/Protect (Physical Defense, OPSEC, COMSEC, COMPUSEC, Counter Intel, and Public Affairs), and Passive/Protect (Physical Security and Hardening).

- Employ is organized into four subsets: Strategic Attack, C2 Attack, Interdiction, and Close Air Support. C2 Attack is new as a distinct entity, and ensures the full incorporation of IW capabilities to disrupt the enemy's information cycle (Observe, Orient, Decide, and Act).
- Enhance includes Air Lift, Air Refueling, Space Lift, Special Operations, and a third new entity called Information Operations, which includes C2, Communications and Computers, Recce, Surveillance, Intelligence, Navigation and Positioning, Combat ID, and Weather Ops).
- Support includes Base Operability and Defense, Logistics, Combat, and On-Orbit.
- To reiterate, this proposed Air Force Doctrine has Information Warfare overlaid on the roles and missions of air power. To ensure that IW receives the appropriate level of emphasis, three new entities have been broken out: Counter Information, C2 Attack, and Information Operations. Therefore, IW will be immediately doctrine-based.
- C2W is too narrow a definition for IW. IW provides more options for traditional target sets, and offers new targets other than C2W. The use of IW and information is vital to Air Power.
- Air Force does not lay claim to IW. Rather, it needs a national focus. Execution of IW objectives needs theater focus and orchestration, and should be done by service components as directed by the CINCs.
- Doctrine today does not go below the Joint Staff level. There need to be clear distinctions between joint functions and the roles of the components.
- The processes for prosecuting IW and other forms of warfare need to be integrated, not separated. There need be no distinction between Lethal and Non-Lethal weapons; an Integrated Target Allocation Process must be used for IW and other weapons.
- Targeting processes need to be reevaluated given the value added of IW in warfare. Concepts to be considered are: Data Bases, Procedures, Assessment and Restrike, Distinctions and Capabilities in Black & White Worlds, and Transition from Peace to War.
- Commercial markets drive IW. The proliferation of off-the-shelf products has made the establishment of technical data bases on a world-wide basis a virtual impossibility. Air Force suggests technology templating to make the problem more manageable.
- Roadmap to the Future
    - Develop Doctrine and Policy
    - Review Programs and Procedures for Focus
    - Training and Education
    - Improve Embedded C4 Security
    - Proposed a Center of Excellence for Modeling Integrated with IW
    - Conduct Legal Assessment

This page intentionally left blank.


TO CERT/FIRST
ARPA
(Acting)
V. Lynn

Organization: Advanced Research Projects Agency

Senior Information Warfare Official:

Dr. Howard Frank, Director, Computer Systems Technology Office, ARPA

Information Warfare Points of Contact:

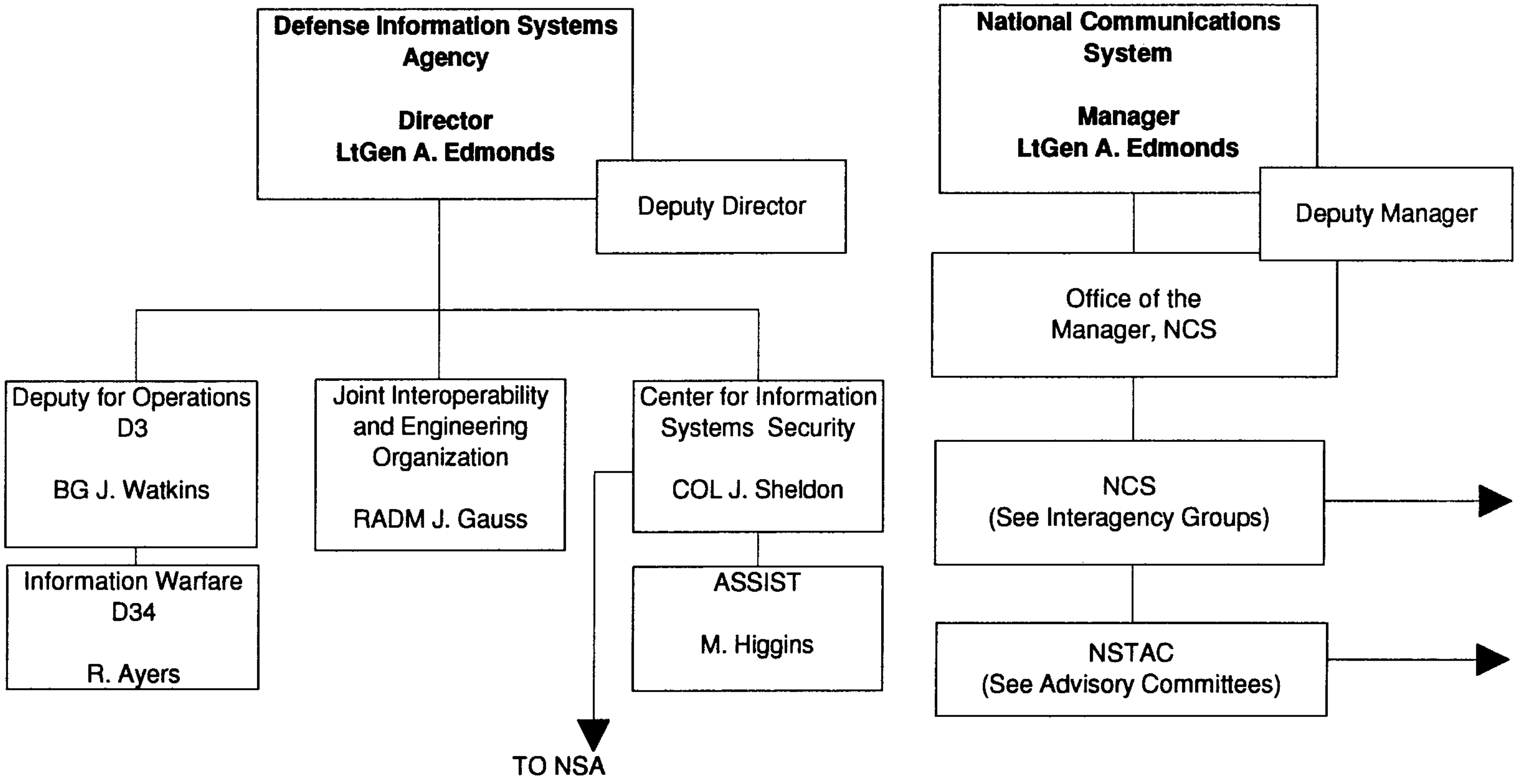
Ms. Theresa Lunt, Program Manager, CSTO, ARPA

Information Warfare Related Missions and Functions:

ARPA is responsible for advanced research in all areas related to information warfare.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- ARPA has established an INFOSEC program and recently solicited proposals from industry and academia on appropriate research initiatives. ARPA is also establishing a Defensive Information Warfare program and is in the process of soliciting proposals on research initiatives for this program.
- Both programs will include research in the following areas:
    * Develop technologies and standards:
        - Scaleable security capabilities.
        - Broaden commercially available security options.
        - Develop technologies for robustness, survivability, attack tolerance, degraded operations, and recovery.
    * Investment areas:
        - Secure networking and technologies - protocols, modular replaceable cryptology-based services, high-speed encryption, key management.
        - Secure computing systems - next generation firewalls, tools for incident response, secure operating systems, secure data interoperability.
        - Assurance technology - security design tools, security testing tools, security metrics and evaluation tools.
        - Technologies for robustness.
- ARPA is also soliciting input on where to invest in R&D, additional participants in R&D, industry interest in establishing joint industry-government test beds, and what the strategy should be for industry acceptance of and transition to new security technologies.
- ARPA is also attempting to determine the proper roles of industry and government - what does industry expect, what is industry willing to do, what standards for security and vulnerability would industry be willing to accept.


Defense Information Systems Agency
Director
LtGen A. Edmonds
Deputy Director
Deputy for Operations
D3
BG J. Watkins
Information Warfare
D34
R. Ayers
Joint Interoperability and Engineering Organization
RADM J. Gauss
Center for Information Systems Security
COL J. Sheldon
ASSIST
M. Higgins
TO NSA
National Communications System
Manager
LtGen A. Edmonds
Deputy Manager
Office of the Manager, NCS
NCS
(See Interagency Groups)
NSTAC
(See Advisory Committees)

Organization: Defense Information Systems Agency (DISA)

Senior Information Assurance Official:

LTG Al Edmonds, Director, DISA

Information Assurance Points of Contact:

Bob Ayers, Chief, Information Warfare Division (D34), Directorate of Operations (D3)
COL John Sheldon, Director, Center for Information Systems Security (CISS)
Mike Higgins, Chief, Automated Systems Security and Incident Support Team (ASSIST), CISS

Information Assurance Related Missions and Functions:

DISA's information warfare responsibilities are based on the following directives:

- Department of Defense Directive 3222.4, Electronic Warfare (EW) and Command and Control and Communications Countermeasures (C3CM), July 31, 1992, which charged the Director, DISA, to "... ensure that DISA architectures consider EW, ECCM, and C3CM."

- Defense Management Review Decision (DMRD) 918, September 1992, designated the Director, DISA, as the "central manger" of the DII.

- Department of Defense Directive 8000.1, Defense Information Management Program, October 27, 1992, which tasked the Director, DISA, to "... in consultation with the Directors of the Defense Intelligence Agency and the National Security Agency, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

- Department of Defense Directive TS 3600.1, Information Warfare, December 21, 1992, which assigned responsibility to the Director, DISA, to "... ensure the DII contains adequate protection against attack."

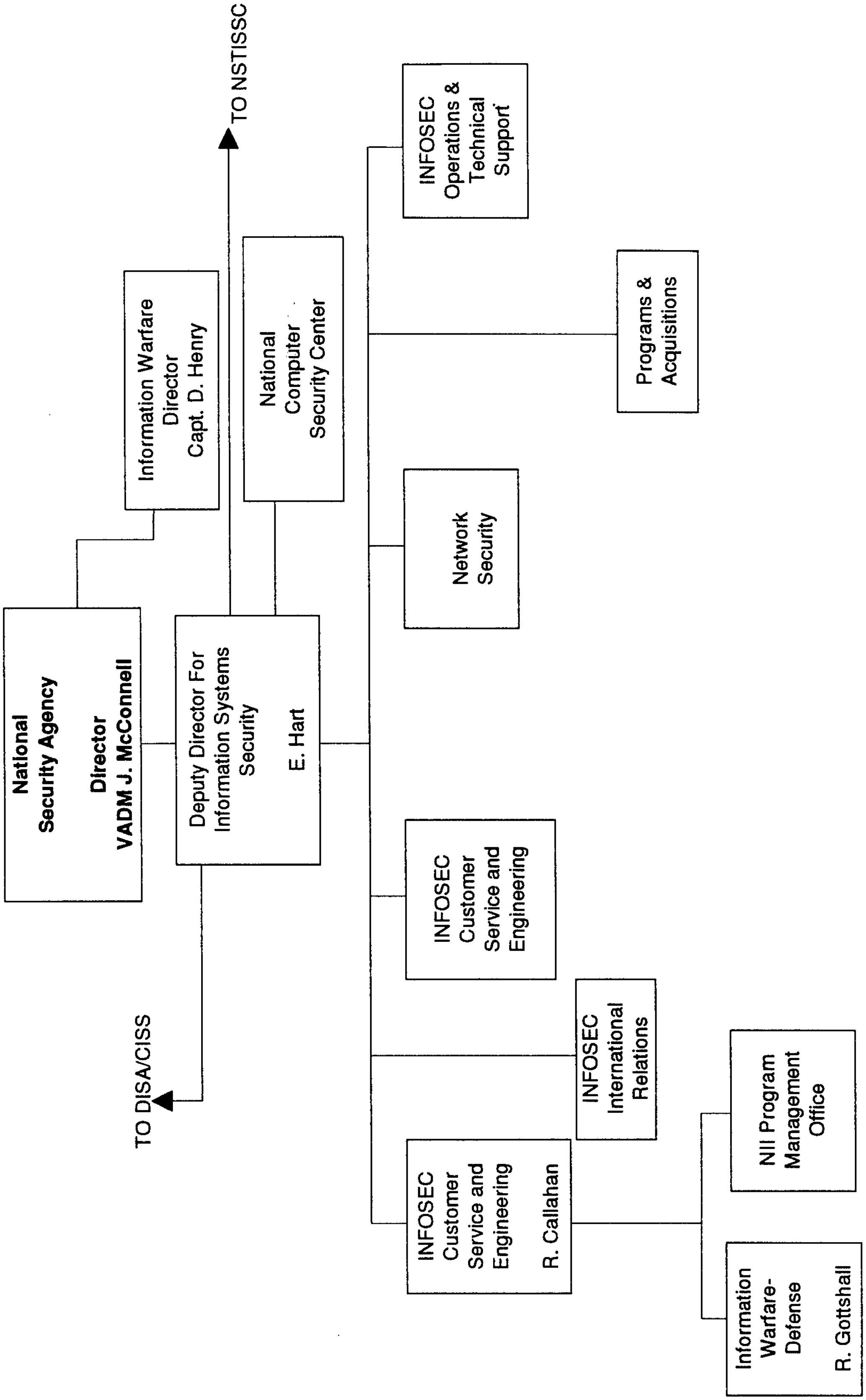
- Chairman of the Joint Chiefs of Staff Memorandum of Policy (MOP) Number 30, Command and Control Warfare, 8 March 1993, which tasked the Director, DISA, to "... assess the vulnerabilities of ... defense information systems..." and to "maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities."

These policy directives form the basis of and provide the authority for actions by the Director, DISA, to protect the DII.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Associations/interagency groups related to computer crime:
  - * Federal Computer Investigators Committee
  - * High Technology Criminal Investigative Association
  - * Interpol
- DIW efforts are hamstrung by current legal structure which prohibits an active defense (tracing perpetrators beyond first node, prohibitions on use of polymorphic code). DoD can't do its job if it can't chase the intruders. Privacy Act impacts on DIW. 1994 Crime Bill forces DoD to show intent to harm in order to pursue perpetrators.
- The legislative proposals being developed by DoJ will help the telecommunications industry. It is not clear how much it will help the Federal Government and other industries.
- DoD is charged with protecting and defending the United States (Title 10) but can't perform this mission on the electronic battlefield because of Posse Commitatus. Situation even more critical when involving efforts to help U.S. corporations overseas -- not clear what information can be passed to whom.
- Clearly need a national policy in the area of information. Must identify who is responsible for what. Recent PRD on organized crime highlighted the impact of computer crime and has sensitized the President's National Security Advisor to computer crime.
- Real issue is how to get industry buy-in into the process. Would help if we knew how to measure the threat.
- Consider the nature of the battlefield (cyberspace). No geographic boundaries, no political boundaries or entities, no temporal boundaries, few laws, little law enforcement, uncertain ownership (of information), little identity, no definitions.
- Security structure is incongruent with IW issues -- the structure focuses on information content rather than the information infrastructure.
- IW is a business practice, not an organizational structure.
- Don't attempt to define things -- might provide wrong focus. Language is inadequate to describe cyberspace. We use a sensory-based language to describe how we count, feel, see. This language is not adequate to help us understand cyberspace. We may also need special tools.

This page intentionally left blank.


National Security Agency
Director VADM J. McConnell
Information Warfare Director Capt. D. Henry
Deputy Director For Information Systems Security
E. Hart
TO NSTISSC
TO DISA/CISS
National Computer Security Center
INFOSEC Operations & Technical Support
Programs & Acquisitions
Network Security
INFOSEC Customer Service and Engineering
INFOSEC International Relations
INFOSEC Customer Service and Engineering
R. Callahan
NII Program Management Office
Information Warfare-Defense
R. Gottshall

Organization: National Security Agency

Senior Information Warfare Official:

Mr. Ed Hart, Deputy Director for Information Systems Security

Information Warfare Points of Contact and Areas of Interest:

CAPT Dave Henry, USN, Director of Information Warfare
CAPT Al Ross, DDO: G42, IW Support Center
Dennis Chiari, DDT: K15
Roger Callahan, DDI: V1
Nick Piazzola, X8
Dr. Clint Brooks, Equities

Information Warfare Related Missions and Functions:

Internal Roles and Responsibilities: CAPT Henry reports to the Director, NSA for Information Warfare issues. He has broad coordination responsibilities to monitor Information Warfare-related activities in both DoD and non-DoD government departments and agencies. He represents the interests of NSA across the entire spectrum of functional disciplines which impact on Information Warfare.

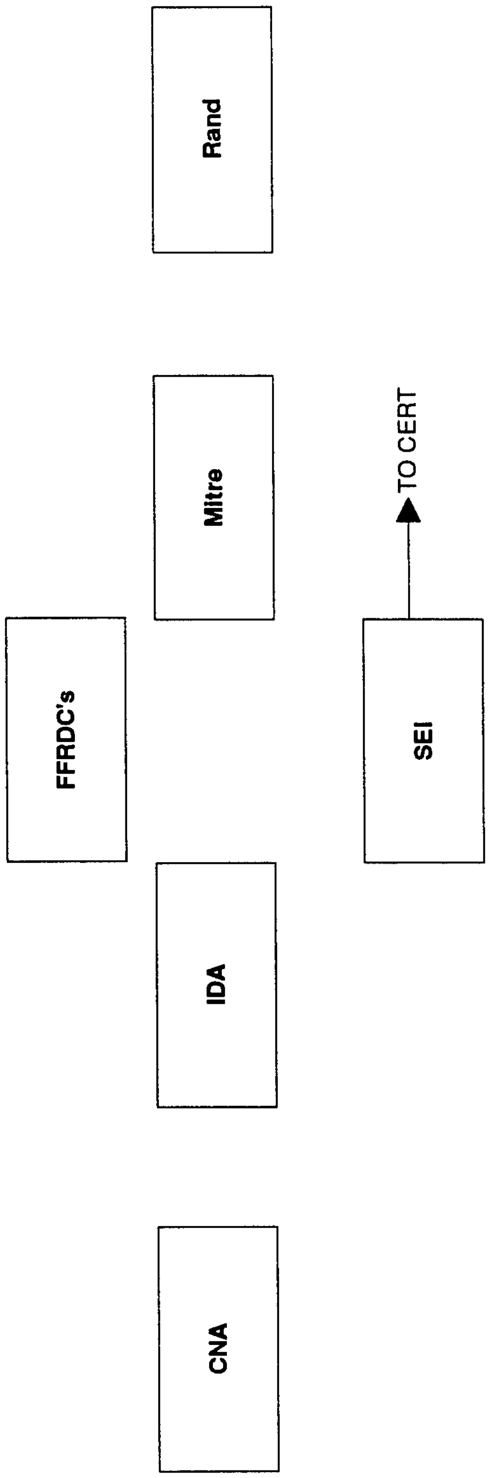
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- On the offensive information warfare side, the concerned elements are: the National Command Authority, the Joint Staff (through the J3), and the warfighting CINCs. Other parties involved in the execution of offensive IW include: Land IW Activity for the Army (under the direction of INSCOM and HQDA) (Col Mike Tanksley); the Navy IW Activity (under NAVSECGRU) (CAPT Greg Blackburn); Air Force IW Center (under AIA) (has several component interests -- San Antonio and SpaceCom); and the Joint Warfare Analysis Center (CAPT Tollhurst). In support of these activities are: NSA, DIA, CIA (CIA performs both support and operations roles in peace and wartime), and DISA (and probably others). In the offensive realm, OSD (C3I) and the Joint Staff have deconfliction responsibilities, while the services build, equip, and maintain forces.
- The defensive information warfare side is not so well defined by definition of responsibilities and the benefits of developmental spending. The same activities are fundamentally involved (from both an operations and support perspective) with the exception of the involvement of J6 instead of J3 on the Joint Staff. The lack of definition is nowhere more apparent (in NSA's eyes) than when viewed through the Computer Security Act of 1987 (P.L. 100-235). The Act stipulates (in part) that government classified information systems-based data is the responsibility of NSA, while government unclassified information is the responsibility of NIST. The difficulty arises when one

considers that 95+% of (classified or unclassified) communications is transmitted across public switches, and the quantity of computers which are in the public domain.

- NSA has developed a concept, called Equities, through which NSA will respond to issues of personal privacy, business privacy, law enforcement, and foreign intelligence with its well-founded systems security expertise. An example of an initiative being promoted to support NSA's role in these issues is the key escrow concept.
- The legal ramifications of IW are significant. On the offensive side, roles are fairly clear after the beginning of hostilities. Before hostilities, deconfliction is a big issue. On the defensive side, P.L. 100-235 is a big issue. What constitutes computer crime? Legal issues at the national level are murky at best. On the international level, it gets murkier.
- Services are starting to get involved in defensive IW, but little has been accomplished to date.
- A Presidential Review Directive (PRD) is being drafted, and may soon be sent to the National Security Council. Among the issues to be addressed: How do DoD and the other agencies interact in IW matters?; How is the NII to be protected?
- There is no overarching national policy on the NII.
- NSA responsibilities include SIGINT, INFOSEC, and OPSEC.
- There is a Professional OPSEC Society which promotes OPSEC in the private sector.
- NSTAC membership has agreed to expand to include other industries.
- IITF's Reliability and Vulnerability Working Group will perform a NII backbone risk assessment. RVWG looking to include industries other than telecommunications.
- No clear definition of who's responsible for information warfare/assurance outside of DoD.
- Must define the infrastructure interdependencies.
- DoD must own and pay for some specified level of security. Question is what is needed
- Need to establish the horizontal coordination mechanisms at various vertical levels.

This page intentionally left blank.


FFRDC's
CNA
IDA
Mitre
Rand
SEI
TO CERT

Organization: Center for Naval Analyses

Senior Information Warfare Official:

Information Warfare Points of Contact:

Dr. Gary Federici

Information Warfare Related Missions and Functions:

CNA provides technical services on a reimbursable basis to the Department of Defense, principally the Department of the Navy. These services include studies, analyses, on-site/deployed support at a senior staff (i.e., CNO) and an operational level. Technical support also includes participation in various wargames conducted at the Naval War College, Newport, RI and other locations.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

CNA studies and analyses in support of Information Warfare have evolved over the years through the various disciplines, such as Electronic Warfare, which are now considered part of Information Warfare. Information Warfare expertise is now an integral part of CNA activities. One such example is support provided to the Naval Studies Board. The product of that Board included the following sections: Role of Information Technology, Information Warfare Weapons and Defenses, Policy & Legal Matters, and Roles and Missions of Information Warfare. CNA has also built a reference library of Information Warfare materials to support their efforts.

Organization: Institute for Defense Analyses (IDA)

Senior Information Warfare Official:

Information Warfare Points of Contact:

Terry Mayfield, Assistant Director, Computer Software and Engineering Division
Bill Barlow

Information Warfare Related Missions and Functions:

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Expect PRD on information assurance to be signed out of DoD shortly. Presidential Decision Directive 35 which addresses national security information should also be signed out shortly.
- Two IDA organizations support IW-related activities, the Systems Engineering Division and the Computer and Software Engineering Division.
- IDA has been asked by J6K to address the role and impact of industry in defensive information warfare. They will also research technologies in or out of DoD which have potential application information warfare.
- IW-related activities include:
  - * Supported JS/J38 in concepts development leading to CJCS MOP 30, Command and Control Warfare.
  - * Analysis of counter-drug operations and security policy development and labeling of information to control dissemination of the counter-drug information.
  - * Estimating value of information and cost of security within DoD. Currently attempting to extend approach to estimate cost of security in private sector.
  - * Ten years supporting NSA in developing trusted computer systems evaluation criteria and evaluating commercial products against the criteria.
  - * Drafting distributed systems evaluation criteria for NSA. Functional portion is completed. Assurance portion being drafted.
  - * Developed security labeling for NSA Common Security Label standard which supports network operations. Counter-drug operational experience was used to add realism to the standard.
  - * Assistance to NSA in drafting, review, and editing of the entire Rainbow series of documents.
  - * Synthesized integrity aspects of INFOSEC into NCSC Technical Reports 79-91 and 101-91.
  - * Supported NSA and DISA in developing certification and accreditation procedures for DoD information systems.
  - * Supported DISA in developing the DoD Goal Security Architecture which identifies where to establish security and the supporting rationale, and in developing the DGSA

Overall Transition Strategy which integrates security functions identified in the DGSA and organizational responsibilities.

- * Support to DISA Center for Standards.
- * In cooperation with NSA and the U.S. Naval Postgraduate School, IDA is establishing a Center of Excellence for Information Security. USNPGS point of contact is Dr. Cynthia Irving.
- * Assisted ARPA is developing the recently released BAA on Information Security and in evaluating the proposals. Approximately 150 proposals were received for the program which begins in FY 96 and will continue for three years. This program will address protection of operating systems, firewalls, intrusion detection, infrastructure protocols, infrastructure vulnerabilities, cryptography, and assurance tools and techniques.
- * IDA will also assist ARPA in the forthcoming (June) release of a BAA for Defensive Information Warfare which will address technologies for a robust information infrastructure (consistency, distributed monitoring, staging of levels of protection, etc.).
- * Assisting the ARPA CSTO in the Information Sciences and Technology (ISAT) Summer Study which is a look at technology opportunities for DIW from the commercial sector. This study will be briefed in August 1995. Will assist ARPA in an interim review of the study to determine impact on the DIW BAA.
- * Have developed and conducted training and education courses on computer security.
- * Operate supercomputing research center in support of NSA. Have additional high performance computing research underway at LaJolla, CA, and Princeton, NJ.
- * Operate a simulation center. Attempting to define how to simulate the effects of IW.

- Identified one central IW issue as cryptography from a technical point of view - when and how to use, alternatives, infrastructures, patents, performance, law enforcement, equities, protection provided. Identified National Science Foundation effort to review cryptology policy.
- Another major issue is the radical restructuring of industry. The traditional providers and users of technology are being merged, acquired, and lost in the efforts to streamline. This will have major implications for any technical infrastructure solution in DIW.

Organization: MITRE Corporation

Senior Information Warfare Official:

Mr. John Woodward, Director of Information Warfare

Information Warfare Points of Contact:

Information Warfare Related Missions and Functions:

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- All INFOSEC assets are assigned as needed on a matrix basis to other parts of MITRE needing assistance. Civil INFOSEC plus AFC3 INFOSEC Division totals about 200 people.
- TRANSCOM stated at a recent training conference in Florida that the command needs policy guidance in the area of information warfare.
- Marty Faga, MITRE, Duane Andrews, SAIC, and other industry representatives are part of an Independent Review Group to advise the Air Material Command's Electronic Systems Center on how to implement its responsibilities for IW.
- MITRE IW support primarily provided to USAF (ESC, AFIWC). Also provide support to NSA. Some support to NIST provided by the Civil INFOSEC organization.
- MITRE Corporation Organizational Structure:
    - MITRE-Corporate
        - Director, Information Warfare
        - MITRE-Environmental
        - MITRE-FAA
        - MITRE-DoD
            - CISS
            - Washington C3 (McLean)
            - AFC3 (Bedford)
                - Electronic Combat
                - INFOSEC Division (Woodward, Associate Technical Director)
        - Civil INFOSEC
- MITRE provides a full range of information security support to DoD to include research, prototyping, product assessment and evaluation, security engineering and acquisition support, and vulnerability analysis.

Department of Defense
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Rank	Service	Title	Telephone	Remarks
Advanced Research Projects Agency			Lunt	Teresa				Program Manager for Info Security	703-696-4469	INFOSEC panelist AFCEA ACCE 95; BAA on INFOSEC; BAA on DIW
Defense Information Systems Agency	Center for Information Systems Security	ASSIST	Higgins	Michael	R				703-692-0250	INFOSEC panelist AFCEA ACCE 95; GCCC
Defense Information Systems Agency	Center for Information Systems Security		Sheldon	John		COL	USA	Commander	703-756-7934	
Defense Information Systems Agency	Deputy Director for Operations (D-3)	Information Warfare Division (D-34)	Ayers	Robert				Division Chief	703-607-6801	
Defense Information Systems Agency	DoD Regulatory Counsel-Telecommunications		Smith	Carl				Chief	703-607-6759	
Defense Information Systems Agency			McCumber	John		Capt	USAF			Has written INFOSEC articles
Defense Nuclear Agency	Springfield Research Facility		Levine	Donald					703-321-0008	National Defense Infrastructure Survivability Study
Department of the Air Force	Air Force Information Warfare Center (AFIWC)	Computer Threat Division (OSKC)	Lemmon	David	P		USAF	Computer Threat Analyst	210-977-3412	
Department of the Air Force	Air Force Information Warfare Center (AFIWC)		May			Maj	USAF		210-969-3550	
Department of the Air Force	Air Force Information Warfare Center (AFIWC)		McCarly	Jim		LtCol	USAF			
Department of the Air Force	Air Force Information Warfare Center (AFIWC)	AIA	Morgan	F.				Commander		Source - SIWS, Also Commander, Joint C2 Warfare Center
Department of the Air Force	Air Force Information Warfare Center (AFIWC)		Osterloh	Robert		Col	USAF	Commander		
Department of the Air Force	Air Force Information Warfare Center (AFIWC)		Tweed	Amy	E	Capt	USAF	Program Manager		
Department of the Air Force	Air Force Office of Special Investigations	Computer Crime Investigations	Christy	Jim				Director		
Department of the Air Force	Computer Emergency Response Team								210-977-3156	
Department of the Air Force	Electronic Systems Center	Directorate of Intelligence and Information Warfare	Szarek	William (Buzz)	J	Capt	USAF			Participates in C4I-Pro discussion group
Department of the Air Force	HQ USAF/SCX	Plans, Policies, and Resources	Bracher	Phillip	E	Maj Gen	USAF	Director	703-695-4440	
Department of the Air Force	USAF Pentagon Communications Agency	Systems Security Requirements Branch, Security Directorate	Boline	Wayne	L	Lieutenant	USAF	Chief	703-697-9088	2nd Int'l Conf on IW, Jan 95 participant
Department of the Air Force	USAF Special Operations Command (AFSOC)		Ash	Mathew	B	Captain	USAF	Chief of Long Range Strategy	904-884-2408	
Department of the Air Force	USAF Special Operations Command (AFSOC)	HQ AFSOC/XPPD	Morrow	Janice	M	Major	USAFR	Chief of Information Warfare Strategy	904-884-2408	
Department of the Air Force			Fiegenbaum	Ed				Chief Scientist		Source - SIWS, AI Expert, Tasked by CSAF to find out everything about IW
Department of the Air Force		Operations XOX	Linhart	Bob		Maj Gen	USAF			
Department of the Air Force		IN	Michael	Ray			USAF		703-695-7817	
Department of the Air Force			Miller	Chuck					703-697-1312	
Department of the Air Force		Air War College	Stein	George						Source - SIWS
Department of the Air Force		Air Command and Staff College	Warden	John		Colonel	USAF	Commandant		Source - SIWS
Department of the Air Force		Operations, XOXD	Wean	Andy		LtCol	USAF			Source - SIWS, Doctrine
Department of the Air Force			Wheeler	Greg		Col	USAF		703-697-8044	
Department of the Air Force		Air Force Doctrine Center	Williams	Wayne		LtCol	USAF			Source - SIWS, AF Manual 1-1, IW Concept Paper
Department of the Air Force		General Counsel	Zeahner	Mike						Source - SIWS, Attorney

Department of Defense
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Rank	Service	Title	Telephone	Remarks
Department of the Army	4th Psychological Operations Group		Jones	Jeff		COL	USA	Commander		Source - SIWS
Department of the Army	Army Counterintelligence Center	902d Military Intelligence Group	Swicegood	Andrew	M		USA	Intelligence Operations Specialist	301-677-3002	ACCE Conference; Coming up to speed on DIW responsiblities.
Department of the Army	DCSOPS DAMO-OD	Land Information Warfare Activity	Tanksley	Mike		COL	USA	Commander		Source - SIWS, Former J33 Division Chief, Colocated with USAINSCOM
Department of the Army	Information Warfare Office	HQDA (DAMO-FD)	McDowell	William	M		USA		703-756-1452	
Department of the Army	Intelligence and Security Command		Tong	Jeffrey	A	Major	USA	Product Manager, Information Warfare	703-756-1460	
Department of the Army	ISMO		Loranger	Phillip					703-696-8070	
Department of the Army	LIWA		Hudson	Tom		LTC	USA		703-706-1069	
Department of the Army	ODISC4	Information Systems Security Office	Brown	Michael	F	LTC	USA	Deputy Director	703-697-1474	
Department of the Army	ODISC4	Army Information Systems Security, Information Security Directorate	Gilreath	Ronald		COL	USA	Deputy Director		
Department of the Army	ODISC4 (SAIS-C4C)	Information Systems Security Office	Willis	Ray				Systems Integrator		
Department of the Army	Physical Operations Division	DCSOPS DAMO-OD	Kaufman	Jim		LTC	USA	Division Chief		Source - SIWS
Department of the Army	TRADOC		Berenson	Paul		Dr.		Science &Technology Advisor		Source - SIWS; Panel member IW track, AFCEA ACCE 95
Department of the Army		Army International Law	Parks	Hayes						Source - SIWS, Rules of Engagement
Department of the Army		DCSOPS DAMO-OD	Scales	Bob		MG	USA			Source - SIWS
Department of the Army		TRADOC	Starry			COL	USA			Source - SIWS, Wrote FM 100-6 Information Operations (22 Jul 94)
Department of the Navy	CNO	N64	Burnette	Gary		LCDR	USN		703-695-0951	
Department of the Navy	CNO	N64	Caldera	Rocco	J	CAPT	USN	Chief		
Department of the Navy	CNO	N3	Schwartzel	Joe		CAPT	USN			
Department of the Navy	CNO	N64	Sherrard	Marty		CAPT	USN	Deputy Chief	703-695-0951	
Department of the Navy	Headquarters, US Marine Corps		Bouldrey			COL	USMC		703-614-3080	
Department of the Navy	Headquarters, US Marine Corps		Robb			LtCol	USMC		703-613-5415	
Department of the Navy	Headquarters, US Marine Corps	C4I	Wiedower			Major	USMC		703-614-4221	RR
Department of the Navy	Naval Command, Control, and Ocean Surveillance Center	Research, Development, Test and Evaluation Division	Ruptier	George				C3I/IW Analysis	619-553-2991	NCCOSC owns Navy C3I and IW technical facilities/labs.
Department of the Navy	Naval Security Group	Naval Information Warfare Activity	Blackburn	Greg		CAPT	USN	Commander	202-764-0599	To be relieved by CAPT Tom Daley, Summer, 95
Institute for Defense Analysis (IDA)	Computer and Software Engineering		Mayfield	Terry				Assistant Director	703-845-6602	
Joint Comand and Control Warfare Center	JCCWC-DV		Gordon	Edward	F	CAPT	USN	Vice Director	210-977-2071	
Joint Comand and Control Warfare Center			Casciano	John	P	Brig Gen	USAF	Commander		Dual Hatted as Cdr Air Intelligence Agency; Maj Gen Select
Joint Comand and Control Warfare Center			Moore	Ed		CAPT	USN	Deputy Commander		
Joint Command and Control Warfare Center			Swart	William	R			Science Advisor/Technical Director	210-977-2071	
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Gravell	William		CAPT	USN	Chief	703-614-2918	
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Hogan	Billy		LTC	USA		703-614-5990	IW policy and training
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Luzwick	Perry		Major	USAF		703-697-8896	Multilevel security
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Napoliello	Mike		LTC	USA		703-614-7813	IW technology

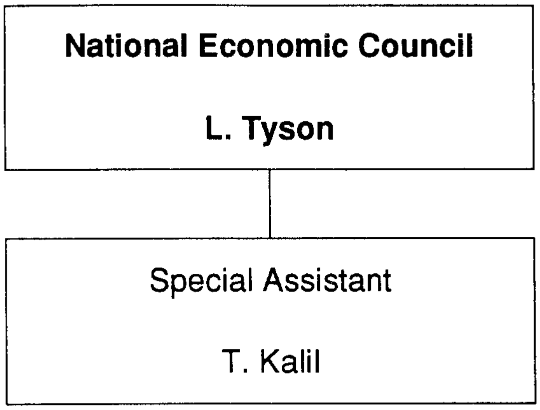
Department of Defense
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Rank	Service	Title	Telephone	Remarks
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Spano	Steve		Major	USAF		703-697-1199	IW assessments and contracts
Joint Staff	C4 Systems Directorate (J-6)	Information Warfare Division (J6K)	Youngs	Dianna		Lt Col	USAF		703-614-7815	COMSEC
Joint Staff	Legal Counsel to the CJCS		Sharp	Gary		Major	USMC		697-1137	Lawyer; Has the J-6 account
Joint Staff	Legal Counsel to the CJCS		Terry	James	P	Colonel	USMC	Legal Counsel to the CJCS	697-1137	Operational experience; Discussions on IW w/ NSA General Counsel
Joint Staff	Legislative Affairs		Farrar	Jay		LTC			614-1777	No IW POC at this time; will work w/ J6K A/O if requested
Joint Staff	Operations Directorate (J3)	Information Warfare/Special Technical Operations Division	Deaver	William	N	CAPT	USN	Chief		
Joint Staff			Roesen			CDR	USN			Has worked on international agreements
Mitre			Woodward	John				Director of Information Warfare	617-271-3647	Mitre Hayes - 883-3616, Associate
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Alger	John		Dr. or COL	USA (Ret)	Director	202-287-9330 Ext. 365	
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Barriteau	Brad				Professor	703-287-9330	
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Carabello	John				Dean		Cochaired IW track at AFCEA ACCE 95
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Czerwinski	Tom				Professor	202-287-9343	
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Giessler	Fred		Dr.		Professor	202-287-9330 Ext. 362	
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Kuehl	Daniel	T			Professor	202-287-9330 Ext. 366	Member on AFIWC PAT on IW
National Defense University	Information Resources Management College	School of Information Warfare and Strategy	Rudolph	Earl	C	CDR	USN	Professor	202-287-9330	
National Defense University			Rokke			LTG		President	202-287-9401	
National Security Agency	General Counsel		Lee	Ronald				General Counsel	688-6705	
National Security Agency	General Counsel	Information Systems Security	Marshall	Richard	H. L.	Lt Col	USAF	Assistant General Counsel	301-688-6017	Well versed in legal environment of IW, particulalry NSA's charter for COMSEC monitoring and testing.
National Security Agency	General Counsel		Prettyman	George				Assistant General Counsel	688-6705	Has worked with Carl Smith. R. Lee is the NSA General Counsel
National Security Agency	Information Systems Security Programs Group		Baggett, Jr.	Charlie	C			Chief		Panelist INFOSEC track, AFCEA ACCE 95
National Security Agency	Information Warfare		Henry	David		CAPT	USN	Director	301-688-5131	
National Security Agency	ISSO	INFOSEC Customer Service and Engineering	Callahan	Roger						Contact LtCol Bill Toney, 301/688-7288
National Security Agency	National Computer Security Center								301-859-4371	
National Security Agency	Office of INFOSEC Research and Technology		Moorcones	Joseph	J			Chief		INFOSEC panelist AFCEA ACCE 95
National Security Agency	Public Affairs		Keller	Barbara					410-766-8729	Provided Rainbow Series Documents
Office of the Secretary of Defense (OSD)	ASD(C3I)		Hotard	Doug		COL	USAF	Director, Information Warfare	703-693-2157	Source - SIWS
Office of the Secretary of Defense (OSD)	ASD(C3I)	DASD(C3I) Information Security	Valeri	Barbara				Director	703-695-8705	
Office of the Secretary of Defense (OSD)	ASD(SOLIC)		Roberts	Jim		SES				Source - SIWS
Office of the Secretary of Defense (OSD)	Legislative Affairs		Shields	Bill		CDR	USN		694-9115	Tracks advanced technology, R&D issues.
Office of the Secretary of Defense (OSD)	OASD (C3I)	Intelligence Program Support Group	Freestone	Bill		Col	USA (Ret)		703-602-5873	
Office of the Secretary of Defense (OSD)	OASD(C3I)	Information Assurance (DIW)	Spencer	John					703-614-0623	
Office of the Secretary of Defense (OSD)	USD (Policy)		Dryden	Sheila						Source - SIWS

Department of Defense
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Rank	Service	Title	Telephone	Remarks
Office of the Secretary of Defense (OSD)	USD (Policy)	Infrastructure Policy	Greene	Brent		Capt	USN	Chief	703-614-2616	
Office of the Secretary of Defense (OSD)	USD (Policy)		Hadley	Dan				Attorney		Source - SIWS, Attorney
Office of the Secretary of Defense (OSD)	USD (Policy)	Office of Net Assessment	Marshall	Andrew				Director		Quote: Information Age will spark a "military revolution."
Office of the Secretary of Defense (OSD)	USD (Policy)		Verga	Pete				Military Aide to Mr. Wells	703-697-0286	Source - SIWS
Office of the Secretary of Defense (OSD)	USD (Policy)	Policy Support	Wells	Linton				Director	703-697-0286	Source - SIWS, Mil Aide Pete Verga
Office of the Secretary of Defense (OSD)			Paige	Emmett		LTG (Ret)	USA	Assistant Secretary of Defense (C3I)	703-695-0348	
Office of the Secretary of Defense (OSD)			Williamson	Charles						
RAND			Arquilla							Source - SIWS
RAND			Johnson	Dana						Source - SIWS
RAND			Ware	Willis					310-393-6432	FFRDC; CSSPAB
	Department of Defense Security Insititute		Grau	Joseph						
	Department of Defense Security Institute		Fischer	Lynn	F					
			Baxter	Larry						Legal guidance from Navy Studies Board study on IW
			Crayton	Al					703-695-9066	Source - SIWS, IW Doctrine
			Green	Toni						SIWS Student; Possibly going to J6K

This page intentionally left blank.



National Economic Council

L. Tyson

Special Assistant

T. Kalil

Organization: National Economic Council (NEC)

Senior Information Assurance Official:

Hon. Laura Tyson, Assistant to the President for Economic Security

Information Assurance Points of Contact:

Mr. Tom Kalil, NEC Staff

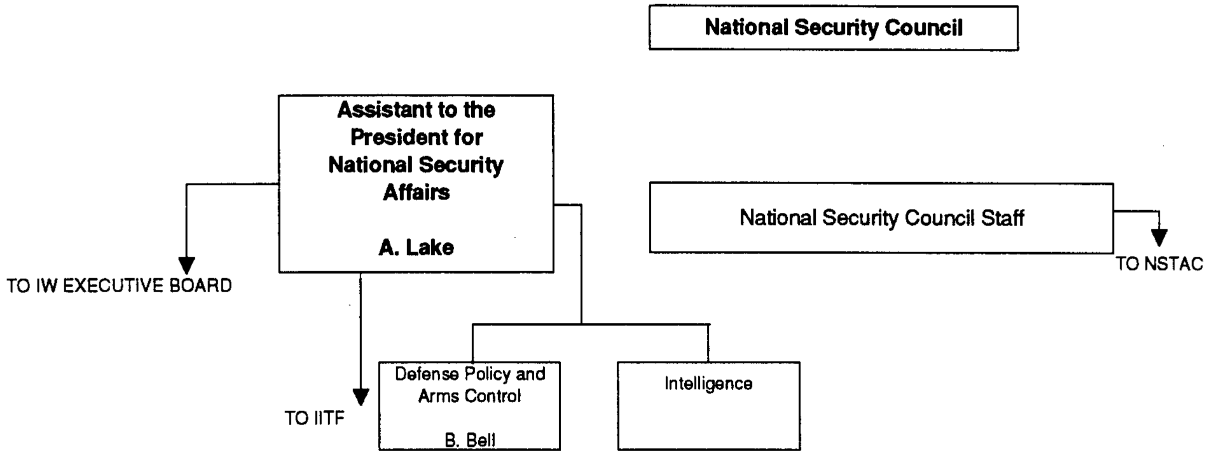
Information Assurance Related Missions and Functions:

The NEC is responsible for coordinating all domestic and international economic policy.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

The NEC and the Office of Science and Technology Policy collaborated on planning for the Information Infrastructure Task Force, which was established by Vice President Gore and is chaired by Hon. Ron Brown, Secretary of Commerce. Mr. Kalil continues to be actively involved in IITF activities.

Mr. Kalil is also involved in cryptology policy issues such export controls and key escrow considerations.


National Security Council
Assistant to the President for National Security Affairs
A. Lake
National Security Council Staff
TO NSTAC
TO IW EXECUTIVE BOARD
TO IITF
Defense Policy and Arms Control
B. Bell
Intelligence

Organization: National Security Council

Senior Information Assurance Official:

Bob Bell, Defense Policy and Arms Control, NSC Staff

Information Assurance Points of Contact:

Colonel Steve Jones, Director for Defense Policy, NSC Staff
Bruce Pease, Director for Intelligence, NSC Staff
Ed Appel, Director for Counterintelligence, NSC Staff

Information Assurance Related Missions and Functions:

Members are the President, the Vice President, the Secretary of State, and the Secretary of Defense. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff are statutory advisors for intelligence and military matters, respectively.

The Secretary of the Treasury, the U.S. Trade Representative, the Chief of Staff to the President, and the Assistants to the President for National Security Affairs and Economic Policy are invited to all meetings of the Council.

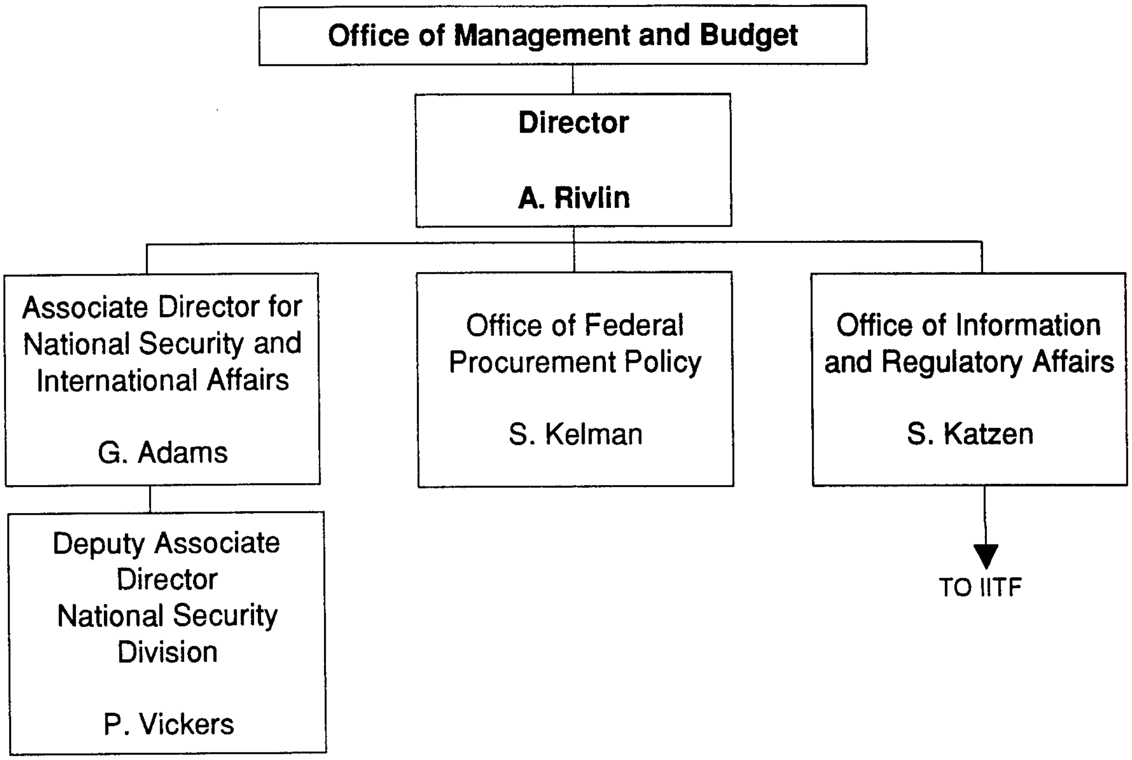
The Council advises and assists the President in integrating all aspects of national security policy as it affects the United States -- domestic, foreign, military, intelligence, and economic -- in conjunction with the National Economic Council.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Defense Policy and Arms Control Office headed by Bob Bell has the lead for information operations and assurance.
- The Intelligence Office headed by George Tenet handled the Clipper and data encryption issues. This office (Ed Appel) also has oversight over the U.S. Security Policy Board.
- OMB is actively involved in the issue, particularly Ms. Sally Katzen's group. The NSC legal staff has not been actively involved to date. The National Economic Council should be involved. OSTP (Mike Nelson) is concerned about how the National Information Infrastructure will affect or be affected by the Global Information Infrastructure. OSTP (Jane Wales) will also be very active in the information assurance issue.
- New national security strategy emphasizes economic security - many implications to this in terms of roles and responsibilities for information assurance.
- NSC will not begin a formal review of the information assurance issue until it receives the draft Presidential Review Decision (PRD) from DoD. DoD's difficulty in getting the PRD out is symptomatic of the difficulties ahead.

- President's National Security Telecommunications Advisory Committee (NSTAC) has asked for a focal point for information assurance. An interim response to the NSTAC Chairman Esrey is currently being coordinated within the EOP.
- Bottom line regarding need for national policy on information is, "Tell me what you cannot do because of a lack of national-level policy guidance."

This page intentionally left blank.


Office of Management and Budget
Director
A. Rivlin
Associate Director for National Security and International Affairs
G. Adams
Office of Federal Procurement Policy
S. Kelman
Office of Information and Regulatory Affairs
S. Katzen
Deputy Associate Director National Security Division
P. Vickers
TO IITF

Organization: Office of Management and Budget, Executive Office of the President

Senior Information Assurance Official:

Sally Katzen, Administrator, Office of Information and Regulatory Affairs

Information Assurance Points of Contact:

Rhebe Vickers, Deputy Associate Director, National Security Division
Bruce McConnell, Chief, Office of Information and Regulatory Affairs
Ed Springer, Office of Information and Regulatory Affairs

Information Assurance Related Missions and Functions:

The Office of Management and Budget evaluates, formulates, and coordinates management procedures and program objectives within and among Federal departments and agencies. Some of its primary responsibilities are to assist the President in developing and maintaining effective government, assist in developing efficient coordinating mechanisms to expand interagency cooperation, assist the President in preparing the budget, assist in developing regulatory reform proposals and programs for paperwork reduction, especially reporting burdens of the public, to plan and develop information systems that provide the President with program performance data, and to improve the economy, efficiency, and effectiveness of the procurement process.

The Office of Management and Budget establishes Federal policy for the security of Federal automated information systems in OMB Circular No. A-130. Appendix III of the Circular requires Federal agencies to establish computer security programs and sets minimum requirements for such programs. The circular applies to the activities of all agencies of the Executive Branch. Issued in 1985, a revised Appendix III was recently released for review and comment. National security information and national security emergency preparedness activities are subject to additional regulations under appropriate directives and executive orders.

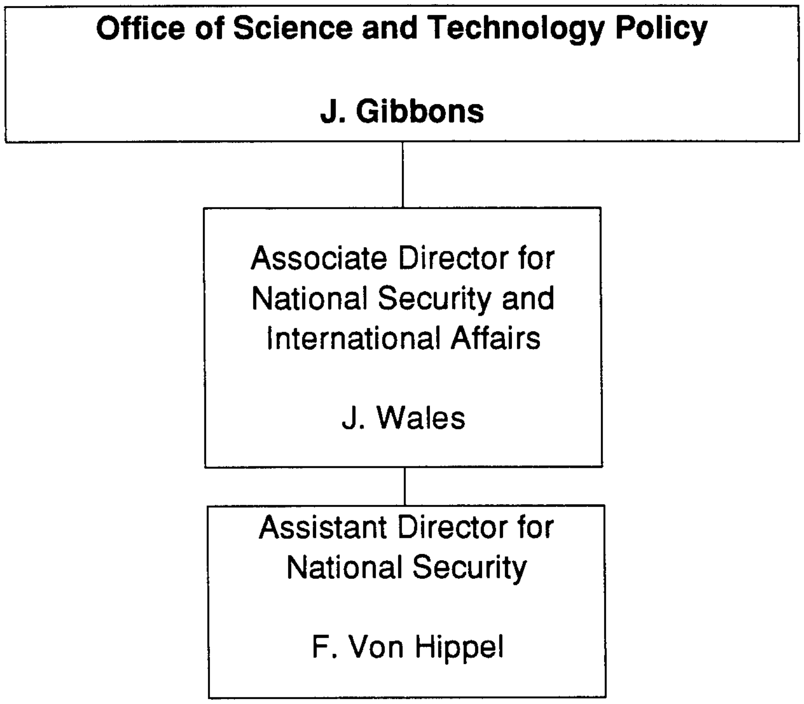
OMB Circular No. A-130, Management of Federal Information Resources, is issued pursuant to OMB's authorities under the Paperwork Reduction Act, (44 U.S.C., Chapter 35), the Privacy Act (5 U.S.C. 552A), the Chief Financial Officers Act (31 U.S.C. 3512 et seq), the Federal Property and Administrative Services Act (40 U.S.C. 759 and 487), the Computer Security Act (40 U.S.C. 759 note), the Budget and Accounting Act (31 U.S.C. Chapter 11), Executive Order 12046 and Executive Order 12472.

The provisions of Executive Order 12958, classified National Security Information established the Information Security Oversight Organization to oversee the implementation of Executive Order 12958. The ISOO was transferred from GSA to OMB last year.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- There is increased citizen awareness of information technology and of government information technology activity.
- Policy areas of concern include: intellectual property rights, software protection privacy, security (NII Security Plan due out shortly).
- National Performance Review implementation underway through Government Information Technology Services (GITS).
- IT management:
  - Congress wants change.
  - Centralized rules don't mesh with new Congress desire for decentralization.
  - Will need performance measures and means for rapid resolution of disputes.
  - A-130 revisions nearly complete.
  - Need some form of interagency management.
- Security:
  - A-130 will update security appendix.
  - Trying to adapt security policy to technology change.
  - Must do risk-based management, measure value of information.
  - Need to be concerned about the insider threat!
  - Must stress individual awareness, reduced documentation, individual responsibility.
  - Integrity important part of process.
  - U.S. Security Policy Board will be a part of process.
  - Must have a definition of national security information.
  - Must have agreement before policy deliberations.
  - Clipper was sprung on the community. Need open dialog before deciding on a solution.
  - Forthcoming release of Revised A-130 and dialog will provide example of how to coordinate security issues. New version will address open and internetworked environment. Will also address management controls.
- Recommend use of Federal Register for comments.
- Investments:
  - Budget - Bad news: worse than last year; Good news: better than next year's!
  - OMB publishing guide on how to justify IT investments.

This page intentionally left blank.



Office of Science and Technology Policy

J. Gibbons

Associate Director for
National Security and
International Affairs

J. Wales

Assistant Director for
National Security

F. Von Hippel

Organization: Office of Science and Technology Policy

Senior Information Assurance Official:

Ms. Jane Wales, Associate Director for National Security and International Affairs, OSTP
Dr. Mike Nelson, Special Assistant for Information Technology, OSTP

Information Assurance Points of Contact:

Lee Johnson, National Security Division, OSTP

Information Assurance Related Missions and Functions:

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 (Public Law 94-282). OSTP's responsibilities are to:

- Advise the President in policy formulation and budget development on all questions in which science and technology (S&T) are important elements.
- Lead an interagency effort to develop and implement S&T policies and budgets that are coordinated across Federal agencies.
- Articulate the President's S&T policies and programs to the Congress, and address and defend the need for appropriate resources.
- Foster strong partnerships among Federal, State, and local governments, and the scientific communities in industry and academe.
- Further international cooperation in science and technology activities.

OSTP's Director also serves as the Assistant to the President for Science and Technology. In this capacity, he manages the National Science and Technology Council (NSTC) and the President's Committee of Advisors on Science and Technology (PCAST).

The NSTC is a Cabinet council, chaired by the President, that acts as a "virtual" agency for science and technology to coordinate the diverse parts of the Federal R&D enterprise. PCAST is a committee of distinguished individuals appointed by the President to provide private sector advice in the S&T policy making process.

OSTP is led by a Director and four Associate Directors, all of whom are Presidentially-appointed and Senate-confirmed. OSTP is organized into four divisions:

Science Division

The Associate Director for Science leads the White House effort to ensure that: 1) the United States continues to maintain global leadership in science, mathematics, and engineering research; and (2) science continues to provide support for the successful resolution of some of the most important problems in the areas of health, agriculture, the economy, energy, social well-being, education, and national security. The Division focuses on maintaining a broad Federal research program that advances the frontiers of knowledge, is based on excellence, strongly coupled to education, and supportive of critical national goals.

Technology Division

The Associate Director for Technology leads the White House effort to develop and implement federal policies for harnessing technology to serve national goals such as global economic competitiveness, environmental quality, and national security. The Division's priorities include: redirecting the U.S. space and aeronautics program, including the space station; sustaining U.S. leadership in defense technology while increasing the focus on dual use and civilian technologies; advancing technologies for education and training for all learning environments; and facilitating development and adoption of advanced manufacturing technologies and advanced computing and communications technologies.

Environment Division

The Associate Director for Environment leads the White House efforts to: 1) ensure a sound scientific and technical underpinning for environmental policies, and 2) develop an interagency R&D strategy for environment and natural resource issues.

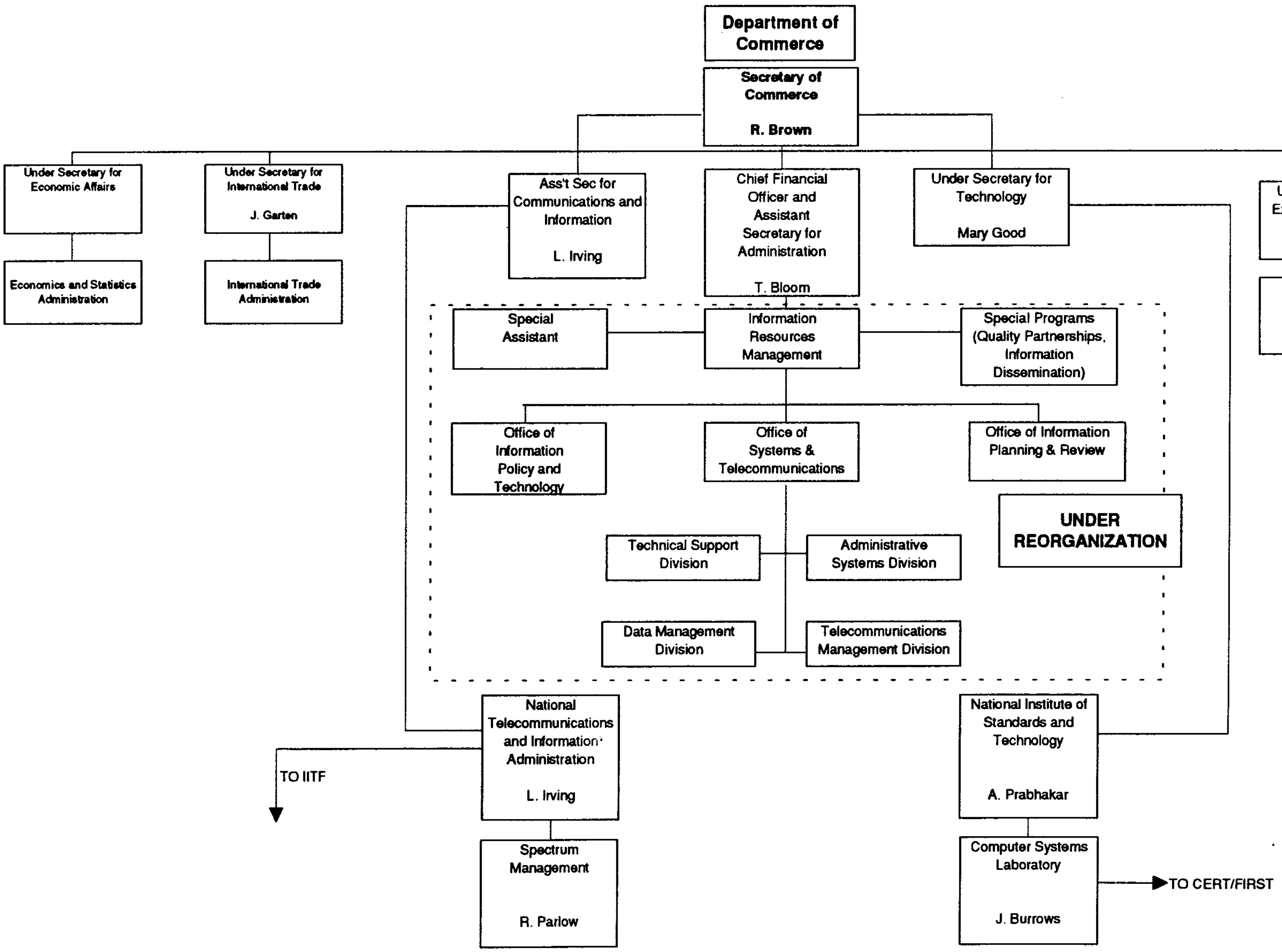
National Security and International Affairs Division

The Associate Director National Security and International Affairs leads the White House effort to use science and technology in the service of our national security, and to shape and coordinate international cooperation in S&T. The national security agenda includes: defense technology investments in an era of downsizing; technical aspects of arms control and nonproliferation policy; technology transfer and related export control policies; and intelligence technology. The international agenda includes: using U.S. leadership in S&T to support U.S. foreign policy objectives; strengthening American S&T in the context of an increasingly interdependent world; using international cooperation in S&T to support economic goals; and enhancing international cooperation in large-scale science programs.

OSTP also plays a key role in formulating a national strategy to continue the development and evolution of the National Information Infrastructure, working closely with the Information Infrastructure Task Force on a number of issues.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


Department of Commerce
Secretary of Commerce
R. Brown
Under Secretary for Economic Affairs
Economics and Statistics Administration
Under Secretary for International Trade
J. Garten
International Trade Administration
Ass't Sec for Communications and Information
L. Irving
Chief Financial Officer and Assistant Secretary for Administration
T. Bloom
Under Secretary for Technology
Mary Good
Under Secretary for Export Administration
W. Reinsch
Bureau of Export Administration
Special Assistant
Information Resources Management
Special Programs (Quality Partnerships, Information Dissemination)
Office of Information Policy and Technology
Office of Systems & Telecommunications
Office of Information Planning & Review
UNDER REORGANIZATION
Technical Support Division
Administrative Systems Division
Data Management Division
Telecommunications Management Division
National Telecommunications and Information Administration
L. Irving
TO IITF
Spectrum Management
R. Parlow
National Institute of Standards and Technology
A. Prabhakar
Computer Systems Laboratory
J. Burrows
TO CERT/FIRST

Organization: Department of Commerce (DoC)

Senior Information Assurance Official:

Thomas R. Bloom, Chief Financial Officer and Assistant Secretary for Administration

Information Assurance Points of Contact:

Alan Balutis, Deputy Assistant Secretary for Administration
Tom Scott, Office of Budget and Finance, Information Security Policy

Information Assurance Related Missions and Functions:

The Department of Commerce encourages, serves, and promotes the Nation's international trade, economic growth, and technological advancement. It offers assistance and information to increase America's competitiveness in the world economy; administers programs to prevent unfair foreign trade competition; provides social and economic statistics and analyses for business and government planners; provides research and support for the increased use of scientific, engineering, and technological development; grants patents and registers trademarks; develops policies and conducts research on telecommunications; and provides assistance to promote domestic economic development. It carries out these responsibilities in the Office of the Secretary and its operating units, a selected number of which are described below.

The Bureau of Export Administration is responsible for directing the Nation's export control policy in accordance with the Export Administration Act and the Export Administration Regulations. The Bureau maintains a Commerce Control List of sensitive or dual-use items including software and scientific and technical data which is maintained for national security purposes, to prevent the items from reaching proscribed countries, and for various foreign policy objectives. It exercises control by processing export license applications, conducting foreign availability studies to determine when products should be decontrolled, and enforcing U.S. export control laws.

The International Trade Administration is responsible for promoting world trade and for strengthening the international trade and investment position of the United States. The Bureau of Export Administration and the International Trade Administration were created by law to be separate organizational entities within the Department.

The National Oceanic and Atmospheric Administration mission is to explore, map, and chart the global ocean, to describe, monitor, and predict conditions in the atmosphere, ocean, Sun, and space environment, to issue warnings against impending destructive natural events, and to disseminate long-term environmental information.

The National Telecommunications and Information Administration responsibilities are described in a separate organizational summary.

The Technology Administration is responsible for working with U.S. industry in addressing competitiveness issues. It discharges this role through the Office of Technology Policy by advocating coherent policies for maximizing the impact of technology on economic growth, through the National Institute for Standards and Technology (NIST) by carrying out technology programs with U.S. industry, and through the National Technical Information Service by disseminating technology information. Specific National Institute for Standards and Technology responsibilities are described in a separate organizational summary.

The Under Secretary of Commerce advises the Secretary and other Government officials on matters relating to economic developments and forecasts and on the development of macroeconomic and microeconomic policy. The Under Secretary, as the Administrator of the Economics and Statistics Administration, exercises general supervision over the Bureau of the Census and the Bureau of Economic Analysis. The Bureau of the Census collects, tabulates and published a wide variety of statistical data about the people ant the economy of the Nation. The goal of the Bureau of Economic Analysis is to provide a clear picture of the U.S. economy through the preparation, development, and interpretation of the national income and product accounts, summarized by numerous indicators such as the gross domestic product, input-output accounts, etc.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Standards developed by NIST are released by the Department of Commerce. GSA publishes telecommunications standards developed by the Federal Telecommunications Standards Committee.
- Community should identify and develop a tool set for security which can be implemented as desired by users.

Organization: National Institute of Standards and Technology (NIST), Department of Commerce

Senior Information Assurance Official:

Jim Burrows, Director, Computer Systems Laboratory

Information Assurance Points of Contact:

Ed Roback, Computer Specialist, Computer Systems Laboratory

Information Assurance Related Missions and Functions:

NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. It does this by assisting industry to develop technology to improve product quality, to modernize the manufacturing process, to ensure product reliability, and to facilitate rapid commercialization of products based on new scientific discoveries.

By the Brooks Act of 1965 and the Computer Security Act of 1987, NIST was assigned responsibilities to develop government-wide computer system security standards and guidelines and security training programs for the protection of sensitive unclassified information maintained in federal government computer systems. NIST also administers the Computer System Security and Privacy Advisory Board to advise the Secretary of Commerce, the Director, Office of Management and Budget, the Director, National Security Agency, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs. These responsibilities are carried out by the Computer Systems Laboratory (CSL).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NIST has approximately 35 people and a base budget of $4.5 million augmented by approximately $3.5 million in other agency funding to fulfill the above responsibilities.
- Significant accomplishments include Data Encryption Standard, Digital Signature Standard, Federal Information Processing Standard (FIPS) 86.
- If DoD desires national-level discussions, it must properly frame the issue. Must be able to properly articulate the threat. Must distinguish between hostile and nuisance threats. Recommend DoD have the NSC establish a Blue Ribbon panel to study the relationship of national and economic security and information assurance in general. The panel's findings and recommendations should then be part of an extensive public dialog.
- Debate leading to Computer Security Act of 1987 provides very useful historical perspective. Suggested review of House Government Operations and House Science and Technology Committee reports regarding the legislation.

- Mr. Niel Stillman, leader of the Government-wide Electronic Mail project, issued a request for information in which he asked about using the Defense Message System (DMS) for Government e-mail. Most responses indicated DMS would be overkill in terms of needed protection.
- Must identify some incremental approach which has cost realism. Policy issues for the private sector must be translated into cost.
- NIST administers the Computer System Security and Privacy Advisory Board which was created by Computer Security Act of 1987. Board consists of volunteers. In general, board is not resourced to properly do its job. Its impact to date has been minimal.
- Many of the recommendations made in the NRC report "Computers at Risk" are still valid. Example is recommendation to establish Information Security Foundation.
- CSL is a member of the Global Task Force on Organized Crime.
- The Interagency Working Group on Encryption and Telecommunications is chaired by Mike Nelson of the Office of Science and Technology Policy and Ed Appel of the National Security Council Staff. It includes membership from NIST, NSA, DoJ, FBI, DoS, CIA, Treasury, and others.
- Government Information Technology Service group IT-10 recommended that NIST develop Generally-Accepted Systems Security Practices (GSSP). Stu Katzke is involved in the effort. Expect to publish practices in the near future.
- Information Systems Security Association is also involved in publication of their own GSSP.
- NIST currently provides secretariat for the Forum of Incident Response and Security Teams. Resources are not sufficient.

Organization: National Telecommunications Information Administration (NTIA), Department of Commerce

Senior Information Assurance Official:

Larry Irving, Administrator

Information Assurance Points of Contact:

Dick Parlow, Chief, Office of Spectrum Management
Bill Gamble, Office of Spectrum Management

Information Assurance Related Missions and Functions:

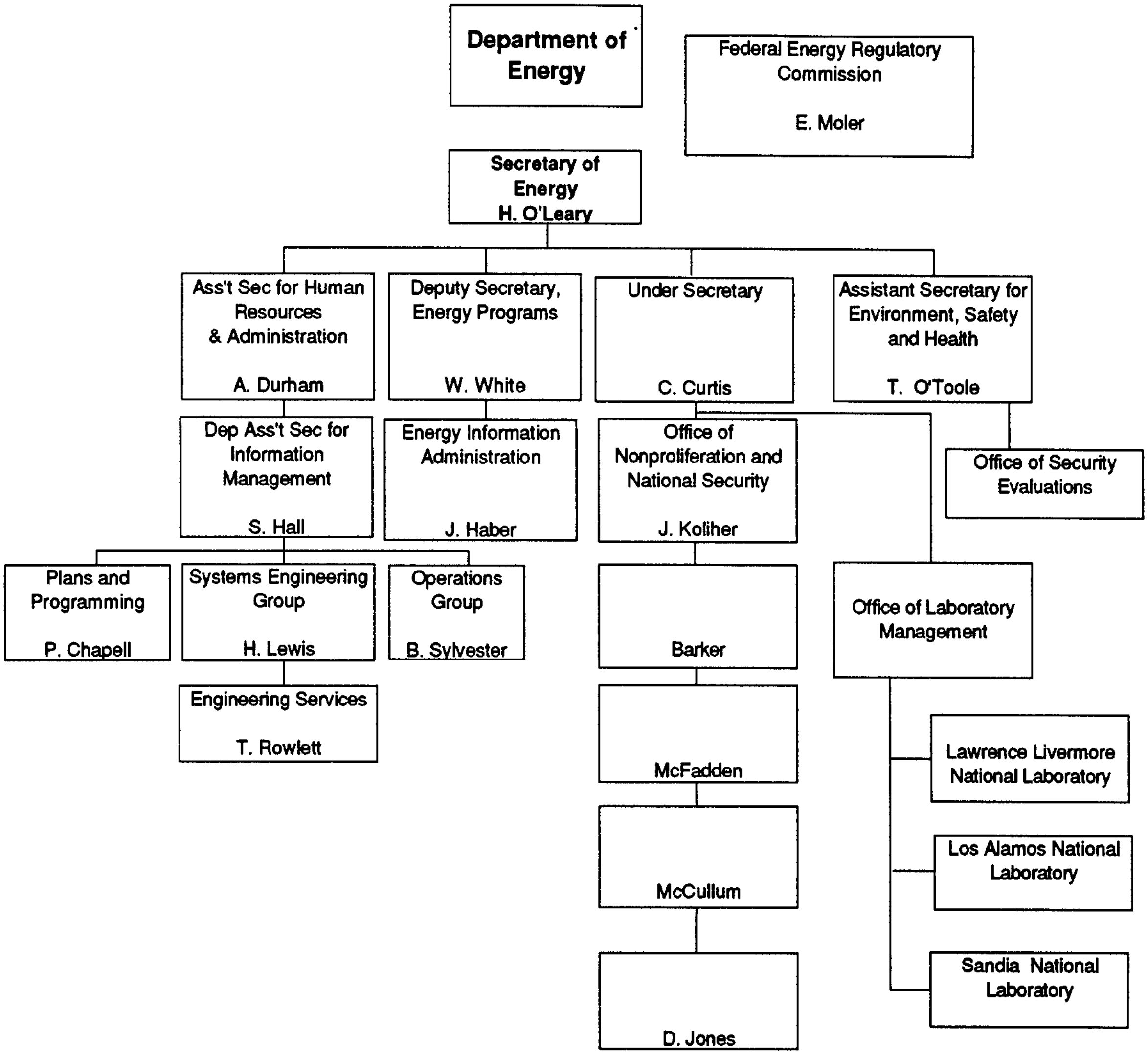
The National Telecommunications and Information Administration responsibilities are to serve as the principal executive branch advisor to the President on telecommunications and information policy, to develop and present U.S. plans and policies at international communications conferences and related meetings, to coordinate U.S. Government positions on communications with the Federal Communications Commission, the U.S. Department of State, and other Federal agencies, to prescribe policies for and managing Federal use of the radio frequency spectrum, to serve as the principal Federal telecommunications research and engineering laboratory through the Institute for Telecommunications Sciences, to provide grants through the Telecommunications and Information Infrastructure Assistance Program (TIIAP) for planning and demonstration projects to promote the development and widespread availability of advanced telecommunications technologies, to provide grants through the Public Telecommunications Facilities Program to extend delivery of public telecommunications services to U.S. citizens and to strengthen the capabilities of existing public broadcasting stations to provide telecommunications services.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NTIA has been a participant in most Information Infrastructure Task Force committees and working groups. NTIA is actively involved in all wireless activities related to IITF.
- NTIA also participates in bilateral activities related to deregulation, opening markets, etc. Other participants include Office of U.S. Trade Representative, International Trade Administration, and DoS.
- The Institute of Telecommunications Sciences at Boulder, CO, does telecommunications research (e.g., propagation characteristics). ITS also participates in standards development for wireline environment.
- NTIA administers Telecommunications and Information Infrastructure Assistance Program, a grant program funded at approximately $28M in FY95, and the Public Telecommunications Facilities Program, a grant program funded at approximately $23M in FY95.

- NTIA has conducted field hearings on universal service and held a symposium on state and local issues related to the NII. Information can be obtained from the NII Advisory Committee Designated Federal Official, Ms. Celia Nogales, 202-482-1835, and from the TIIAP Infrastructure Office, Ms. Laurie Breedon, 202-482-2048.

This page intentionally left blank.


Department of Energy
Federal Energy Regulatory Commission
E. Moler
Secretary of Energy
H. O'Leary
Ass't Sec for Human Resources & Administration
A. Durham
Deputy Secretary, Energy Programs
W. White
Under Secretary
C. Curtis
Assistant Secretary for Environment, Safety and Health
T. O'Toole
Dep Ass't Sec for Information Management
S. Hall
Energy Information Administration
J. Haber
Office of Nonproliferation and National Security
J. Koliher
Office of Security Evaluations
Plans and Programming
P. Chapell
Systems Engineering Group
H. Lewis
Operations Group
B. Sylvester
Barker
Office of Laboratory Management
Engineering Services
T. Rowlett
McFadden
Lawrence Livermore National Laboratory
Los Alamos National Laboratory
McCullum
Sandia National Laboratory
D. Jones

Organization: Department of Energy (DoE)

Senior Information Assurance Official:

Information Assurance Points of Contact:

Tom Rowlett, Director, Engineering Services, Systems Engineering Group, Information Resources Management
Brent Frampton, Computer Security Specialist, Energy Information Administration

Information Assurance Related Missions and Functions:

The Department of Energy provides the framework for a comprehensive and balanced national energy plan throughout the coordination and administration of the energy functions of the Federal Government. The Department is also responsible for energy regulatory programs and a central energy data collection and analysis programs.

The Office of Non Proliferation and National Security safeguards and secures classified information and protects departmental and Department of Energy contractor facilities and installations, manages the Department's Emergency Management System, which responds to and mitigates the consequences resulting from operational, energy, and continuity of Government emergencies.

The Office of Information Resources Management is responsible for development and implementation of policy regarding the protection of sensitive but unclassified information.

The Office of the Assistant Secretary for Environment, Safety, and Health is responsible for independent oversight of nuclear/non-nuclear safety and security laws, regulations, and policies.

The Energy Information Administration is responsible of the timely and accurate collection, processing, and publication of data in the areas of energy resource reserves, energy production, demand, consumption, distribution and technology.

The Federal Energy Regulatory Commission is responsible for setting rates and charges for the transportation and sale of natural gas and for the transmission and sale of electricity and the licensing of hydroelectric power projects.

The Office of Laboratory Management is responsible for institutional policy and oversight functions related to utilization of the Department of Energy's multiprogram laboratories to assure optimum utilization of the Department's laboratory complex for meeting national research and technology development objectives. Organizational summaries for the

Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, and Sandia National Laboratories follow.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Information security responsibilities split in DoE. Office of IRM responsible for unclassified information (to include connections to Internet). Office of Nonproliferation and National Security responsible for classified information.
- Office of IRM currently working on a DoE policy for sensitive unclassified information with primary emphasis on encypherment.
- The Assistant Secretary for Environment, Safety, and Health operates an Office of Security Evaluations which encompasses physical and logical security.
- DOE's ESNet is primary backbone of Internet.
- Office of IRM's Engineering Services organization operates the Computer Incident Advisory Capability (CIAC). They also provide information security assistance visits as requested.
- Must emphasize responsibilities of information owners and hold them accountable.
- Moving away from specific policy directives to guidance.
- DoE owns National Laboratory facilities and products of research. Laboratories are operated by independent activities, such as the University of California.
- Current issues:
  - * Cryptology policy -- MOSIAC, Clipper.
  - * DoE components supporting private sector being asked to use Pretty Good Privacy (PGP).
  - * Need to educate users.

Organization: Lawrence Livermore National Laboratory (LLNL), P.O. Box 808,
Livermore, CA 94551, 505/422-8193

Senior Information Assurance Official:

Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The Computer Security Technology Center (CSTC) is an element of the Computation Organization at the LLNL; it serves the needs of clients in the U.S. Department of Energy (DoE) and other federal agencies. The CSTC delivers solutions to today's information technology security challenges through integration of operations; incident response, product development, and consulting services.

Computer Incident Advisory Capability (CIAC) is an element of the CSTC and is also located at LLNL. CIAC provides computer security free of charge to employees and contractors of the DoE; these services include: incident handling, computer security information, on-site workshops, and computer security consulting. CIAC provides operational incident response and serves as the single point of contact for all DoE incident handling. This team gathers fast-breaking vulnerability and threat information and disseminates it throughout the DoE community. CIAC is also a founding member of Forum of Incident Response and Security Teams (FIRST).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Organization: Los Alamos National Laboratory, Los Alamos, NM

Senior Information Assurance Official:

Information Assurance Points of Contact:

Vance Faber, Group Leader, Computer Research and Applications Group
Charlenne Douglas, Group Leader, Computer and Communications Security Group

Information Assurance Related Missions and Functions:

The computer networks of the LANL are divided into two parts. One part contains the nuclear weapons information and has no connection to the outside world. It cannot be accessed by anyone from outside the laboratory.

The Computer Research and Applications Group builds fraud detection software for many special purpose projects. Most of the group's research tends to be with on-line training and operating modes, adaptive systems, and neural net type systems.

The Network Anomaly Detection Intrusion Reporter (NADIR) system has been running on the laboratory's network since 1989. The goals of this system are detection, deterrence, and accountability. It is an expert system-an automated audit system. The network, all the nodes attached to it, and all the computers have always had the requirements for forming logs and reporting. NADIR has now taken over the task of looking through these logs and detecting anomalous behavior.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Organization: Sandia National Laboratories

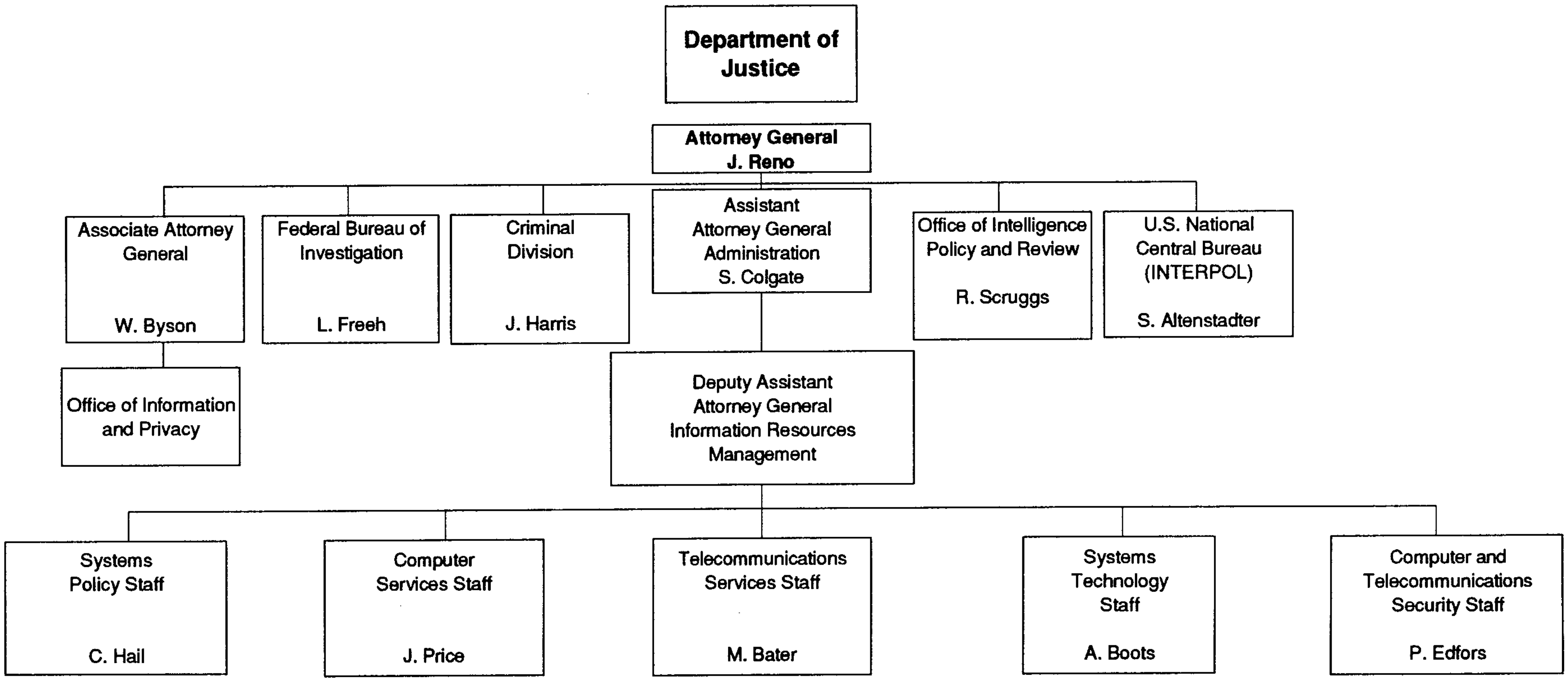
Senior Information Assurance Official:

Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The end of the Cold War era has stimulated DOE's national laboratories to contribute to economic security, synergistic with their public missions in defense, energy, and the environment. Recognizing the complexity of the issues and relationships for industry-led and government partnered enterprises, Sandia's National Industrial Alliances Center has developed and implemented the Prosperity Games in partnership with the National War College, Lawrence Livermore National Laboratories, the Electronics Industries Association, and the American Electronics Association. Under the auspices of the Electronics Subcommittee of the NSTC, the Prosperity Games have provided energy for and assessment of road maps of the technology and policy options related to electronic manufacturing in the United States.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


Department of Justice
Attorney General
J. Reno
Associate Attorney General
W. Byson
Office of Information and Privacy
Federal Bureau of Investigation
L. Freeh
Criminal Division
J. Harris
Assistant Attorney General Administration
S. Colgate
Office of Intelligence Policy and Review
R. Scruggs
U.S. National Central Bureau (INTERPOL)
S. Altenstadter
Deputy Assistant Attorney General Information Resources Management
Systems Policy Staff
C. Hail
Computer Services Staff
J. Price
Telecommunications Services Staff
M. Bater
Systems Technology Staff
A. Boots
Computer and Telecommunications Security Staff
P. Edfors

Organization: Department of Justice (DoJ)

Senior Information Assurance Official:

Stephen R. Colgate, Assistant Attorney General for Administration

Information Assurance Points of Contact:

Roger M. Cooper, Deputy Assistant Attorney General for Information Resources Management
Patricia Edfors, Director, Computer and Telecommunications Security Staff, Information Resources Management, Justice Management Division
Judy Bloom, Acting Deputy Director, Computer and Telecommunications Security Staff, Information Resources Management, Justice Management Division
Scott Charney, Chief, Computer Crime Unit, Criminal Division
Hal Henderschott, Supervisory Special Agent, Economic Crime Unit, White-Collar Crimes Section, Criminal Investigative Division, Federal Bureau of Investigation

Information Assurance Related Missions and Functions:

The Department of Justice serves as counsel for the Nation's citizens. It exercises this primary responsibility through law enforcement, crime prevention, crime detection, prosecution, incarceration, and rehabilitation of offenders.

The Office of Information and Privacy coordinates policy development and Government-wide compliance for the Freedom of Information Act and the Privacy Act.

The Justice Management Division provides assistance to senior management officials relating to basic Department policy for automatic data processing, telecommunications, security, and records management. The Division develops and promulgates Department-wide policies, standards, and procedures for information systems and reviews their implementation. The Division collects, organizes, and disseminates recorded information that is necessary for the Department to carry out its statutory mandate.

The Office of Intelligence Policy and Review advises the Attorney General on all matters relating to the national security activities of the United States. The Office prepares and files applications for surveillance under the Foreign Intelligence Surveillance Act of 1978 and assists all Government agencies by providing legal advice on matters of national security law.

The Antitrust Division is responsible for promoting and maintaining competitive markets by enforcing the Federal antitrust laws and by acting as an advocate of competition within the Federal Government. The Division also represents the United States in judicial proceedings to review certain orders of regulatory bodies such as the Federal Communications Commission.

The Criminal Division develops, enforces, and supervises the application of all Federal criminal laws, except those specifically assigned to other divisions. The Division includes a Fraud Section which directs and coordinates the Federal effort against fraud and white-collar crime, an Internal Security Section which supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology, and a Money Laundering Section. The Division also includes a Computer Crime Unit which is responsible for implementing the Computer Crime Initiative, a five-point program designed to respond to the growing computer crime problem.

DoJ takes a very direct and deep interest in investigating and prosecuting many varieties of computer crime, ranging from intrusions prosecuted under 18 U.S.C. δ 1030 to the communication of threats over networks. DoJ is interested not only in crimes directed against DoJ facilities, but in all violations of federal law. For example, DoJ works closely with the Air Force's Office of Special Investigations and other military components to address attacks against military computer systems.

The Federal Bureau of Investigation is the principal investigative arm of the Department. Priority has been assigned for investigation of the five areas which affect society the most: organized crime/drugs, counterterrorism, white-collar crime, foreign counterintelligence, and violent crime. The Bureau includes an Economic Crime Unit in the White-Collar Crimes Section of the Criminal Investigative Division which investigates computer crime.

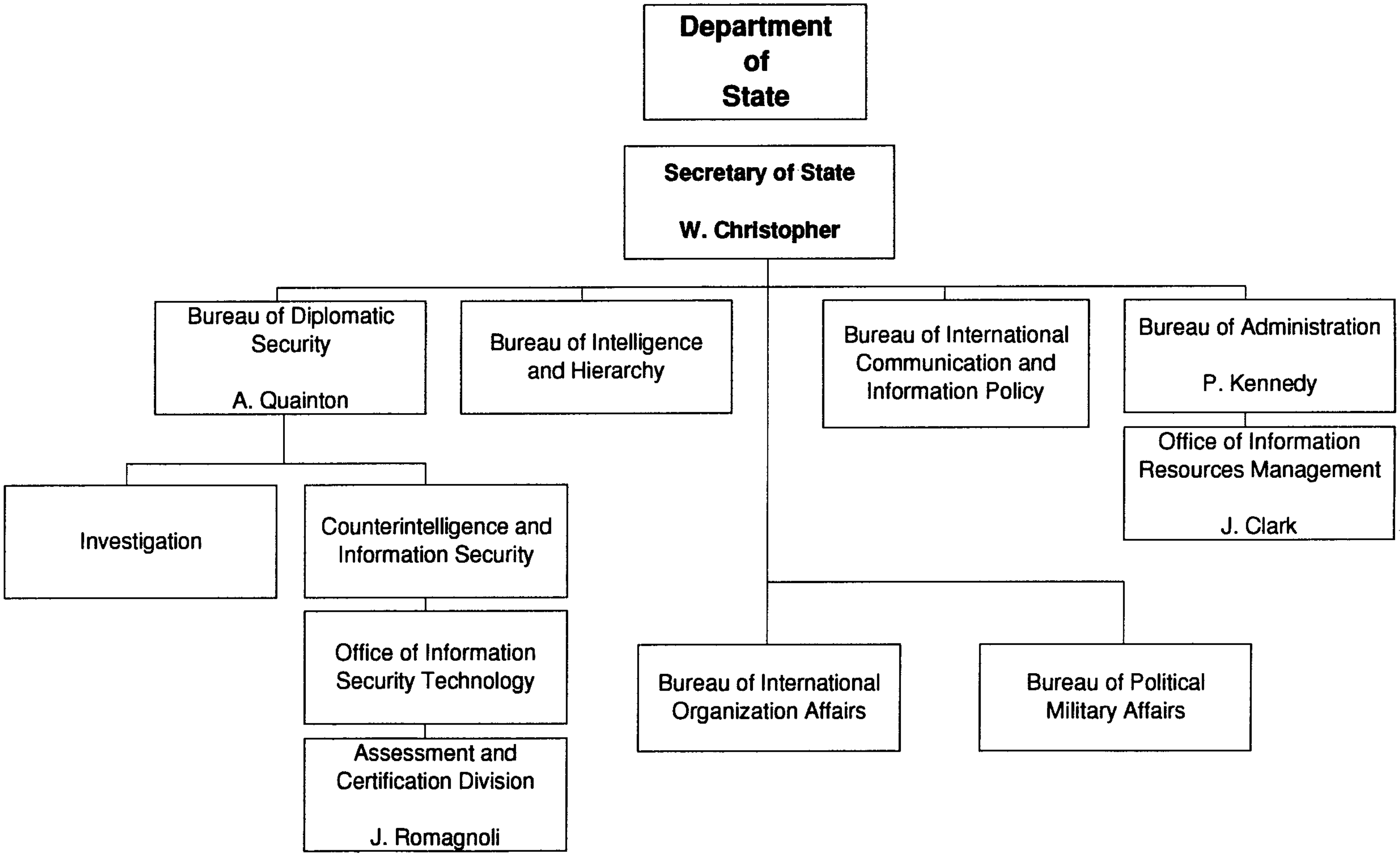
The United States National Central Bureau represents the Unites States in the International Criminal Police Organization (INTERPOL). The Bureau provides an essential communications link between the U.S. police community and their counterparts in the foreign member countries. The Bureau operates through cooperative efforts with Federal, State, and local law enforcement agencies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Department has formed a Computer Security Officers Task Force consisting of the representatives with computer security responsibility from each of the Department's 34 components. Each component Computer Systems Program Manager is responsible for overseeing the activities of Computer Systems Security Officers designated for each system. These systems security officers are full-time or part-time security specialists dependent on the size and sensitivity of the system and its information.
- The Department has unique information protection requirements. On the one hand, it is obligated to share its information with the public and other law enforcement agencies. On the other, the information it holds (evidence, fingerprints, etc.) is very sensitive information. In addition, DoJ must share considerable information with the Judiciary.
- Since DoJ is the principal agency responsible for the federal government's litigation and law enforcement functions, many critical systems and services could be affected: immigration and border controls; criminal investigations; civil suits, many involving large sums of money; control of the federal prison system; litigation and settlements in antitrust cases; litigation of criminal and civil tax cases; matters involving environmental laws; and many others. Specifically in the area of national security, the Department handles many sensitive matters involving intelligence information, including wiretaps

under the Foreign Intelligence Surveillance Act; FBI counter-intelligence investigations; and liaison operations of the FBI, DEA, and others in foreign countries.

- DoJ is in the midst of proposing legislation to further strengthen the laws available to prosecutors in the high-technology area (Sec. 1030 amendments, copyright provisions, Privacy Protection Act, etc.).
- The Criminal Division coordinates closely with many other components inside and outside DoJ: FBI National Computer Crime Squad and the Computer Analysis and Response Team among others to exchange information and develop better legal and tactical approaches to computer crimes. DoJ also coordinates with the Secret Service, IRS, Air Force, Navy, and others.
- Each U.S. Attorney's Office is designating a Computer/Telecommunications Coordinator -- a prosecutor to receive special training in technology issues to act as central point of contact in the office. This program will ensure that agents who have computer-related investigations will have a point of contact who understands the technical matters.
- Information security policy oversight for DoJ is done by the Computer and Telecommunications Security Staff (CTSS). The basis for policy is the existing body of laws and regulations regarding matters with which the various components of DoJ must deal.
- CTSS relies on the DoJ components to provide legal advice and assistance. The staff translates the laws and regulations into technical policy which is then disseminated to the components. Components also write implementing policy which the CTSS periodically reviews for compliance with higher level policy. The policy is also based on existing Executive Branch policy and standards to include NIST standards which are generally not applicable to the current-day distributed computing environment. In general, existing technical policy is centered on the goal of C2 level of protection of information. Implementation of the policy is also complicated by legacy systems and rapid changes in technology.
- Information protection is accomplished by risk management which includes estimates of the viability of the threat and value of the information which must be protected. The threat is a validated threat produced by DoJ. Of note, private detectives and skip tracers (people who located people who default on bail, loans, etc.) as do organized crime, drug trafficking, etc. constitute a significant threat to DoJ information. Additional considerations include the distribution of information and the data upon which the information is based and the aggregation of information.
- Two recent projects represent DoJ best practices in information protection. One is the Counter-Narcotics Information Sharing Project (sometime referred to as Drug X). It was developed in a.totally cooperative manner with two components. It was developed based on extensive discussions with the users. It is a information pointer system and involved developing an architecture based on multiple platforms and information protection requirements. The second project is the Joint Automated Booking System. Its development involved five DoJ components.
- The Department's Justice Performance Review Office recently received approval to establish a Computer Security Technical Laboratory which will include a DoJ Incident Response Service (DOJIRS) and an advanced authentication and encryption test bed. DoJ (CTSS) currently conducts penetration testing of DoJ systems.


Department of State
Secretary of State
W. Christopher
Bureau of Diplomatic Security
A. Quainton
Bureau of Intelligence and Hierarchy
Bureau of International Communication and Information Policy
Bureau of Administration
P. Kennedy
Office of Information Resources Management
J. Clark
Investigation
Counterintelligence and Information Security
Office of Information Security Technology
Assessment and Certification Division
J. Romagnoli
Bureau of International Organization Affairs
Bureau of Political Military Affairs

Organization: Department of State (DoS)

Senior Information Assurance Official:

Anthony C.E. Quainton, Assistant Secretary for Diplomatic Security

Information Assurance Points of Contact:

Jules Romagnoli, Chief, Assessment and Certification Division
John Clark, Director, Office of Information Resources

Information Assurance Related Missions and Functions:

The Department of State advises the President in the formulation and execution of foreign policy. The Department's primary objective in the conduct of foreign relations is to promote the long-range security and well-being of the United States.

The Secretary is the first ranking member of the Cabinet and a member of the National Security Council. The Under Secretary for International Security Affairs is responsible for assuring the integration of all elements of the Foreign Assistance Program and serves as the Chairman of the Arms Transfer Management Group. The Under Secretary is also responsible for international scientific and technological issues, communications and information issues, and technology transfers.

The Bureau of Diplomatic Security provides a secure environment for conducting American diplomacy and promoting American interests worldwide. It assists the Secretary in the formulation and implementation of diplomatic security policy to provide a secure environment for the conduct of American diplomacy and coordinates the exchange of security-related intelligence and operational information among the Department, foreign governments, other U.S. Government agencies, and all law enforcement authorities. The Bureau provides administrative support to the Overseas Security Advisory Council, a Federal Advisory Committee, which provides for regular and timely exchange of information between the private sector and the Department.

The Bureau of Intelligence and Research coordinates the programs of intelligence, analysis, and research and produced intelligence studies and current intelligence analyses.

The Bureau of International Communications and Information Policy coordinates with other U.S. Government agencies and the private sector in the formulation and implementation of international policies relating to a wide range of rapidly evolving communications and information technologies. The Bureau also promotes U.S. telecommunications interests bilaterally and multilaterally.

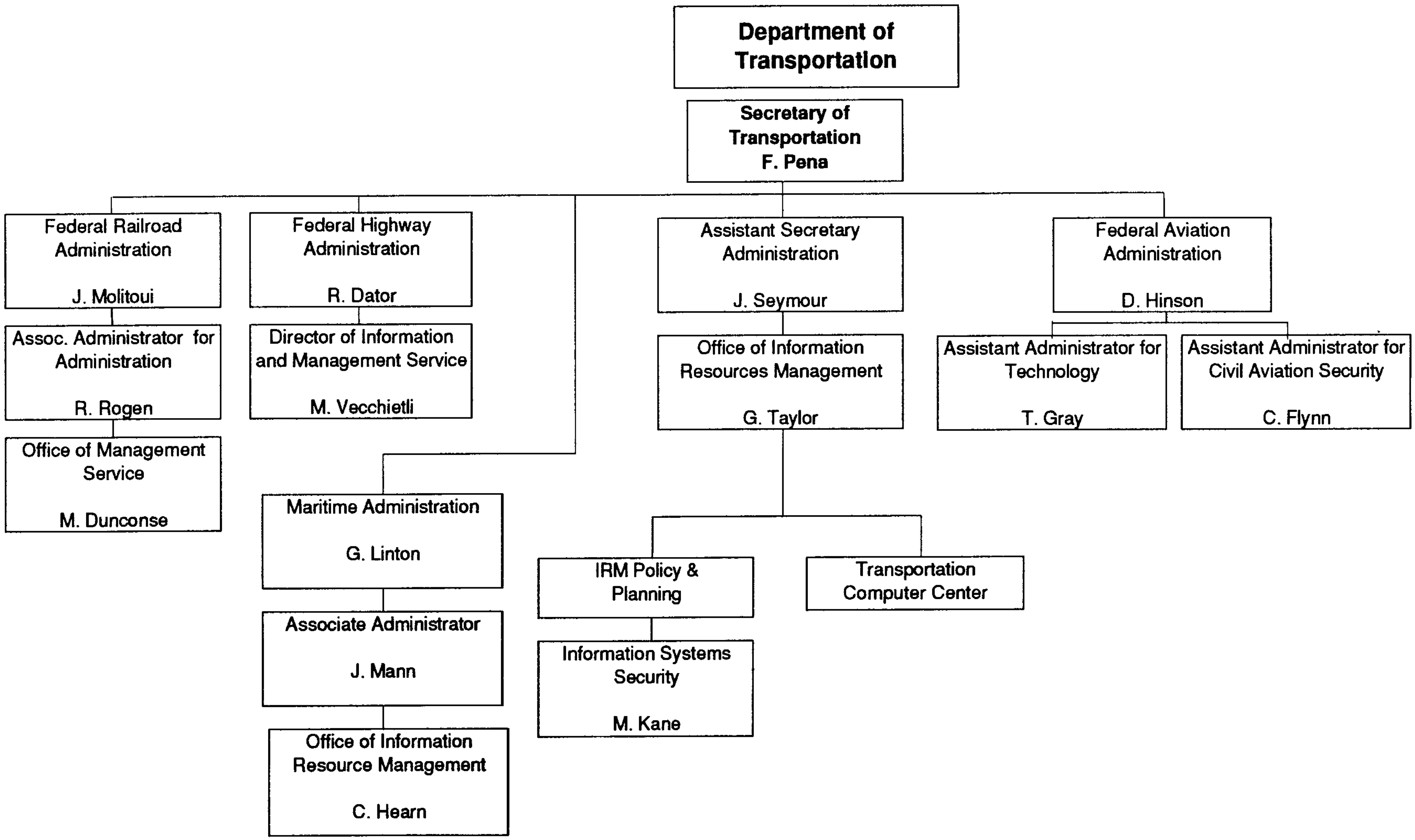
The Bureau of International Organization Affairs leads in the development, coordination, and implementation of U.S. multilateral policy. It formulates and implements U.S. policy toward international organizations with particular emphasis on those organizations which make up the United Nations system.

The Bureau of Political-Military Affairs coordinates policy formulation on national security issues including defense relations and security assistance and export controls. The Bureau's major activities are designed to further U.S. national security objectives by through negotiations, security assistance, curbing proliferation of weapons of mass destruction, and inhibiting adversaries access t military significant technologies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Security administrators looking to Assistant Secretaries to take responsibility for security of systems under their direction.
- DoS uses terms INFOSEC, COMPUSEC and COMSEC.
- Bureau of Diplomatic Security develops and promulgates security policy with the involvement of the other DoS bureaus. Office of Information Security Technology drafts the policy. Office includes responsibility for records security (Ms. Sue Holland) which includes damage assessment and classification of information.
- DS/CIS participates in the NSTISSC. The Deputy Assistant Secretary for CIS is the DoS representative to NSTISSC. Chief, Assessment and Certification Division is the DoS representative to the SAIS and the STSS.
- Operational communications matters are responsibility of Office of Information Management in the Bureau of Administration. Although Office of Information Management and OIST are in different bureaus, they work closely to integrate security early in the systems development process.
- Security policies are articulated in Foreign Affairs Manual.
- The Department is beginning to emphasize risk management. Some savings have already been achieved by moving to risk management. Also trying to identify responsibilities for Assistant Secretaries and pin point ownership of information.
- Assurance goals are always mitigated by operational considerations.
- Major issues are how to incorporate security in open systems architectures, multilevel security, logical management architectures, and networks. Another issue is the fast-paced introduction of technology which seems to out pace the introduction of security technologies. Also need a standard mechanism for sharing information.
- DoS will use DoD Defense Messaging System -- saves on development. DoS does not do any research and development.
- DoS does, however, operate a computer security laboratory which is configured as an embassy node. Lab is used to test all security policies before implementation. Lab simulates all overseas operations for security certification of systems and software. Lab budget is approximately $1.5 million per year. Computer security laboratory used to test, assess, and evaluate security methods. Firewalls used but limit capabilities. Encryption also used but with associated limitations (commonality of equipment, key distribution, limited access, information constraining).
- OIST's education and awareness training are oriented on operational matters, not mandatory security training issues.

This page intentionally left blank.


Department of Transportation
Secretary of Transportation F. Pena
Federal Railroad Administration J. Molitoui
Assoc. Administrator for Administration R. Rogen
Office of Management Service M. Dunconse
Federal Highway Administration R. Dator
Director of Information and Management Service M. Vecchietli
Maritime Administration G. Linton
Associate Administrator J. Mann
Office of Information Resource Management C. Hearn
Assistant Secretary Administration J. Seymour
Office of Information Resources Management G. Taylor
IRM Policy & Planning
Information Systems Security M. Kane
Transportation Computer Center
Federal Aviation Administration D. Hinson
Assistant Administrator for Technology T. Gray
Assistant Administrator for Civil Aviation Security C. Flynn

Organization: Department of Transportation (DoT)

Senior Information Assurance Official:

Mellisa J. Spillenkothen, Assistant Secretary for Administration

Information Assurance Points of Contact:

Michael Kane, DoT Information Systems Security Officer, Office of Information Resource Management

Information Assurance Related Missions and Functions:

The Office of Information Resource Management formulates, prescribes, and assures compliance with telecommunications and automated data processing policy to include information systems security policy.

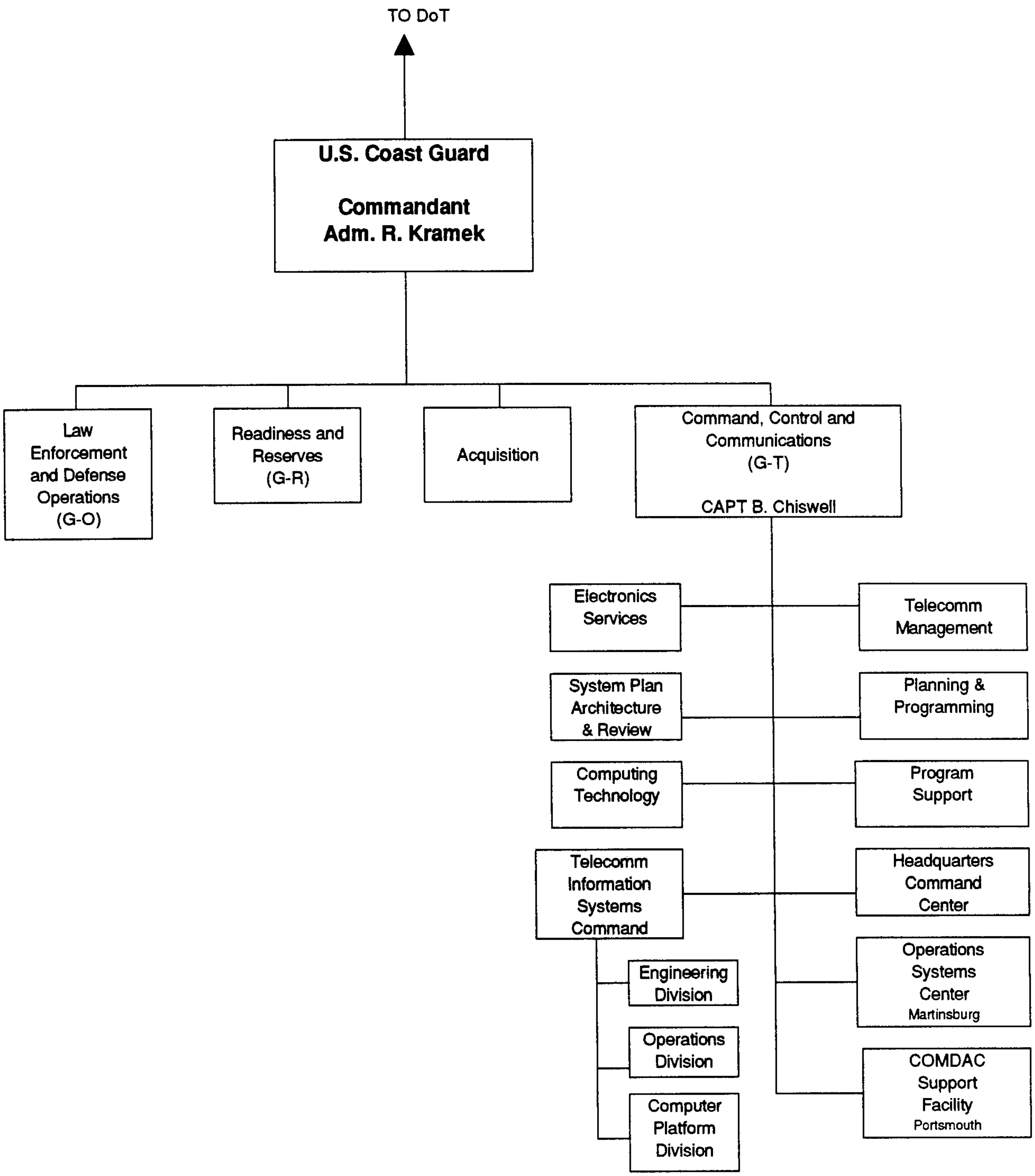
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Departmental Information Systems Security Officer is supported by a staff of two people. Budget is very limited. U.S. Coast Guard (USCG). has three information security staff personnel supported by nine regional officers who perform information security duties as collateral duties. Federal Aviation Administration (FAA) has two information security staff personnel supported by ten regional officers who perform information security duties as collateral duties. Computer centers (Washington, DC, Plano, TX, Cambridge, MA) have full time security officers.
- Reinvention of DoT may result in:
    * Reduction of operating administrations to three -- FAA, USCG, Intermodal Transportation Agency (ITA)
    * Reduction in employees from 105,000 to 50,000 (Including military)
    * Reduction in grant programs from 30 to 3
    * Privatization of air traffic control activities
- Traditional security concerns in DoT are keeping planes in the air, not information security.
- Reduction in grant programs will be accompanied by establishment of "Transportation Banks" for disbursement of monies. This will add enormous security requirements regarding electronic commerce and electronic funds transfer. DOTreas is providing advice on related issues.
- Senior official for information systems security is the Assistant Secretary for Administration, who chairs an Advisory Management Committee (AMC). The Executive Agent for Information Security is Eugene Taylor, the Director of Information Resource Management, who chairs the IRM Advisory Committee (IRMAC). Mr. Kane, the Departmental Information Systems Security Officer, chairs the Subcommittee on Computer Security (SOCS). The AMC and the IRMAC have membership from the

operating administrations. The SOCS has membership from the operating administrations, the Inspector General's Office, and the Computer Centers.

- DoT has been actively conducting oversight reviews to improve security posture. Two years ago, only two of ten operating administrations had information security policies. Will actively continue the reviews, some in the form of self assessments.
- Reviews resulted in establishment of a very good training and awareness program which has been very effective at the end-user level. Still need a similar program to influence management. Will address all OPM and procurement categories and establish performance areas for executives, senior functional managers, IRM personnel, and security personnel.
- DoT uses a departmental security banner on all systems. Also employs a user authorization form for every user.
- Growth of electronic commerce may outrun our ability to adequately secure the commerce. Help from GSA (responsible for the security infrastructure) slow in coming.
- DoT has completed extensive policy-to-standards translations.
- Intend to do penetration demonstration for senior managers in near future.
- DoT concerned about whether significant employee reductions will increase insider threat.
- Kane thinks the Federal Computer Security Program Manager's Forum is productive.
- Information security issues:
  - Multiple e-mail protocols and associated problems.
  - Reinvention of DoT means a new corporate architecture.
  - Which encryption schemes to use (hardware, software, embedded, digital signature standard).
  - Use of conformance standards and how to couple with controls.
- Security must be cost effective and consistent with information being protected. Simple quick-fix, low cost solutions are available.
- Have experienced several penetrations. In one instance, the Intermodal LAN was penetrated within hours of its activation. The perpetrator used the LAN to weave to Maryland and Virginia banks and other sensitive operations.

This page intentionally left blank.


TO DoT
U.S. Coast Guard
Commandant
Adm. R. Kramek
Law Enforcement and Defense Operations (G-O)
Readiness and Reserves (G-R)
Acquisition
Command, Control and Communications (G-T)
CAPT B. Chiswell
Electronics Services
Telecomm Management
System Plan Architecture & Review
Planning & Programming
Computing Technology
Program Support
Telecomm Information Systems Command
Headquarters Command Center
Engineering Division
Operations Systems Center
Martinsburg
Operations Division
Computer Platform Division
COMDAC Support Facility
Portsmouth

Organization: United States Coast Guard

Senior Information Assurance Official:

RADM R. Cianeaglini

Information Assurance Points of Contact:

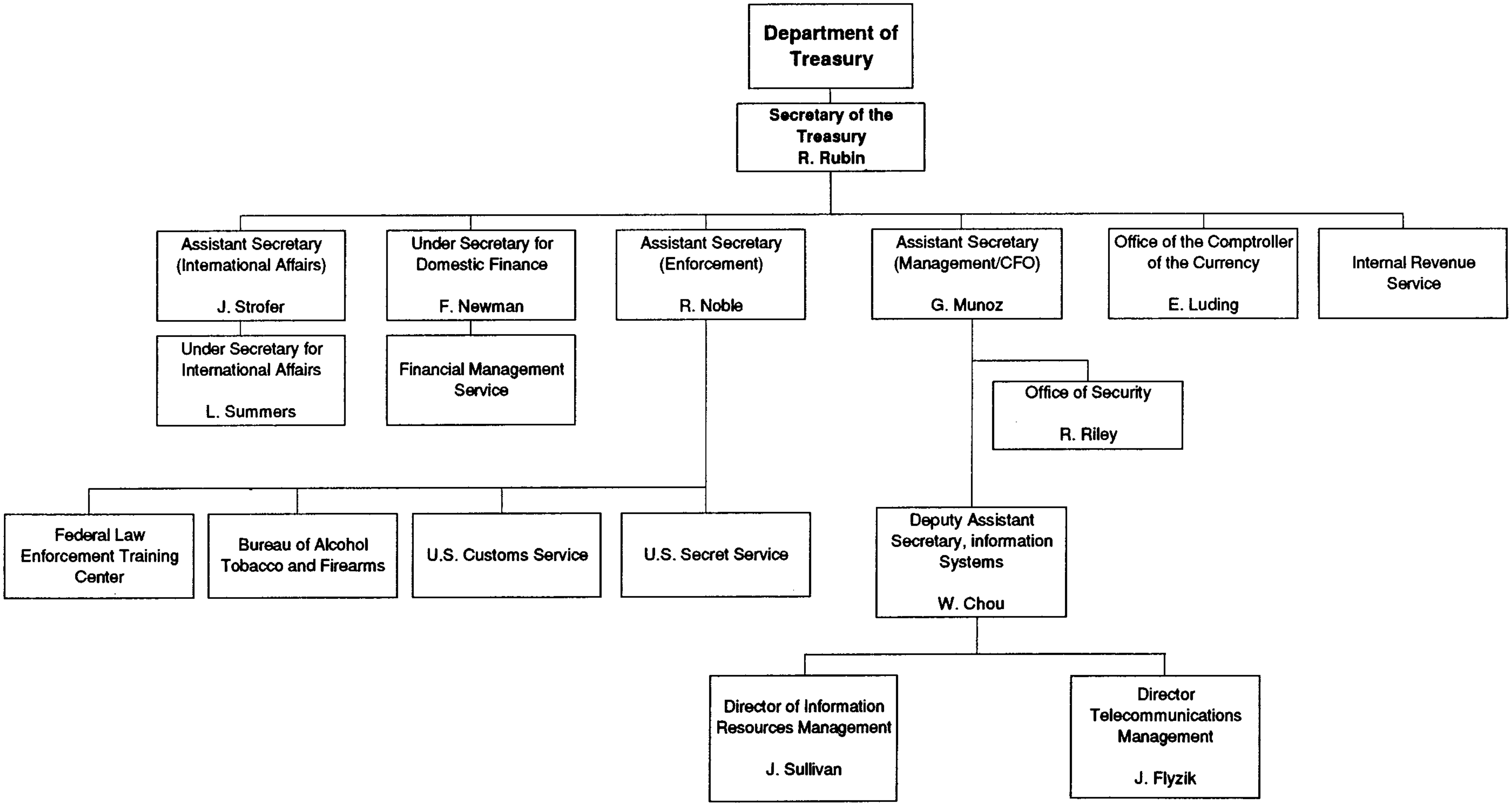
CAPT Fred Edwards
LCDR Mike Inman
CAPT Ben Chiswell
CDR Mike Grimes

Information Assurance Related Missions and Functions:

Law enforcement, navigation, safety, and waterway services. Subordinate to the Navy during time of national emergency.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- With respect to IW, the biggest issue for the Coast Guard is interoperability. Standard operations for the Coast Guard do not mirror DoD when it comes to standardized equipment, procedures, communications assets, or communications paths. The Coast Guard could use access to MILSATCOM, but bandwidth is not available for long range communications. These issues persist even though the Coast Guard has similar requirements for the types of information (real time and near real time) available to DoD entities.
- The Coast Guard supports national security interests but not in the same sense as DoD. The Coast Guard has no organizational definition of IW, and even if it did, it is likely it would differ from the DoD definition. An example of a national security interest which directly involves the Coast Guard is the migrant issue. Migrants are an issue to the State Department, but is not as identifiable with DoD.
- Another key issue which distinguishes the Coast Guard from DoD is a difference in views as to definition of classified information. The tendency is for the Coast Guard to handle, at an unclassified level, information which DoD would treat as classified. This situation arises both as a result of interpretation and expediency in mission execution.
- Attempting to develop an architecture for the Coast Guard to encompass all aspects of C4I and sensors.


Department of Treasury
Secretary of the Treasury R. Rubin
Assistant Secretary (International Affairs) J. Strofer
Under Secretary for International Affairs L. Summers
Under Secretary for Domestic Finance F. Newman
Financial Management Service
Assistant Secretary (Enforcement) R. Noble
Federal Law Enforcement Training Center
Bureau of Alcohol Tobacco and Firearms
U.S. Customs Service
U.S. Secret Service
Assistant Secretary (Management/CFO) G. Munoz
Office of Security R. Riley
Deputy Assistant Secretary, information Systems W. Chou
Director of Information Resources Management J. Sullivan
Director Telecommunications Management J. Flyzik
Office of the Comptroller of the Currency E. Luding
Internal Revenue Service

Organization: Department of the Treasury (Treas)

Senior Information Assurance Official:

G. Munoz, Assistant Secretary (Management) and Chief Financial Officer

Information Assurance Points of Contact:

R. Riley, Director, Office of Security
M. Ferris, Systems Security, Office of Security
W. Chou, Deputy Assistant Secretary (Information Systems)
J. Sullivan, Director, Office of Information Resources,
J. Flyzik, Director, Office of Telecommunications Management

Information Assurance Related Missions and Functions:

The Department of the Treasury formulates and recommends economic, financial, tax, and fiscal policies; serves as financial agent of the U.S. Government; enforces the law; and manufactures coins and currency.

The Secretary serves as the Chief Financial Officer of the Government, Chairman pro tempore of the Economic Policy Council and as U.S. Governor of the International Monetary Fund, the International Bank for Reconstruction and Development, the Inter-American Development and, and the African Development Bank.

The Assistant Secretary (Enforcement) supervises the U.S. Secret Service, U.S. Customs Service, Federal Law Enforcement Training Center, and the Bureau of Alcohol, Tobacco, and Firearms.

The Assistant Secretary is also responsible for the Office of Financial Enforcement, and the Office of Foreign Assets Control. The Assistant Secretary (International Affairs) is responsible for international monetary, financial, commercial, energy, and trade policies and programs.

The Assistant Secretary (Management/Chief Financial Officer) oversees the Department's management programs to include security, management analysis, financial management, and information systems.

The Inspector General is responsible for providing comprehensive, independent, and objective audit and investigation programs to identify and report program deficiencies and improve the economy, efficiency, and effectiveness of operations.

Among other duties, the United States Customs Service is responsible for interdicting and seizing contraband, including narcotics and illegal drugs; detecting and apprehending persons engaged in fraudulent practices designed to circumvent customs and related laws; and, enforcing export control laws and interception of illegal high-technology and weapons exports.

The Bureau of Engraving and Printing is responsible for production of currency and other government documents that, because of their innate value, or some other reason, require security or counterfeit-deterrence characteristics.

The Federal Law Enforcement Training Center is an interagency training center serving over 70 Federal law enforcement organizations. The Center conducts advanced programs in areas such as white-collar crime, use of microcomputers as an investigative tool, and international banking/money laundering. The Center offers selective, highly specialized training programs to State and local officers as an aid in deterring crime.

The Financial Management Service is responsible for working capital management, payments, collections, and central accounting and reporting. As a part of its responsibilities for payments, it issues over 440 million Treasury checks and makes close to 350 million electronic fund transfer payments annually for salaries, wages, goods and services, income tax refunds, and social security and veteran's benefits. Electronic fund transfer payments are accomplished using automated clearinghouses and wire transfers through the Fedline, an encrypted computer-to-computer link with the Federal Reserve System. These Fedline links also use digital signatures to verify the authenticity of the payments.

In addition to its Presidential protection and security responsibilities, the Secret Service is responsible to detect and arrest offenders of laws pertaining to electronic funds transfer frauds, credit and debit card fraud, false identification documents or devices, computer access fraud, and U.S. Department of Agriculture food coupons.

The Office of the Comptroller of the Security regulates national banks.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Treasury has 165,000 employees, operates in a decentralized manner. It relies on OMB and GSA guidance for security of sensitive unclassified information.
- Training alone may not be a cost effective means of improving security.
- Nature of our society is innovation rather than control. Role of government is to protect interests of society as a whole.
- Information assurance discussion seems to focus on vulnerability of telecommunications. Should also be concerned about value-added networks that serve as additional communications infrastructure and which ride on the telecommunications infrastructure.
- New A-130 policy seems to imply that policy should be "let the buyer beware." May be some merit in this approach. Should also establish minimum standards. Treasury participates in several ad hoc industry efforts to develop standards.

- Treasury Department writes very broad policy for Bureau implementation with participation of bureau security experts. Minimum standard practices are included in the Department's security manual.
- Not much budget available for security efforts -- seems to be true of most agencies..
- Department is establishing a very extensive communications and data network, the Treasury Communications System, which will rely on commercial telecommunications.
- Treasury does not do active penetration testing of networks from the Department. Some Bureaus, such as IRS, however, do test their networks.
- FBI mostly concerned about violent crimes. Treasury investigates a lot of computer crime. Bill Friel, Financial Crimes, can provide details.
- Regulation - The Office of the Comptroller of the Currency regulates national banks, the Federal Deposit Insurance Corporation regulates certain banking operations, FEDline used for transfers from government activities to FRS (totally encrypted).
- Treasury has a Telecommunications and Information Security Working Group to coordinate security issues. Information systems security officers do certification and accreditation. Security duties included in job descriptions and categories which identify personnel as being qualified or experienced with security related to certain systems or classes of systems.
- Department, Internal Revenue Service and Financial Management Service participate in developing banking standards.
- May want to check Electronic Funds Transfer Association. Also participate with DISA in development of X.12 standard modifications.
- Wireless architecture and security issues being addressed by Ray Baronet, Secret Service.
- Issues - Civil agencies don't want DoD to specify protection requirements for sensitive unclassified information. This is an area which DoD has neglected and in which civil agencies are very proficient.

This page intentionally left blank.

Executive Branch
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Department of Agriculture	Office of the Chief Financial Officer	Automatic Data Processing	King	Ken		Chief		
Department of Commerce	Computer Systems Laboratory	Computer Security planning and Assistance Group	Toth	Pat		Computer Scientist		
Department of Commerce	National Institute of Standards and Technology (NIST)	Computer Systems Laboratory	Burrows	Jim		Director		
Department of Commerce	National Institute of Standards and Technology (NIST)	Public Affairs	Lennon	Elizabeth			301-975-2832	
Department of Commerce	National Institute of Standards and Technology (NIST)	Computer Systems Laboratory	Martin	Roger	J	Chief, Systems and Software Technology		
Department of Commerce	National Institute of Standards and Technology (NIST)	Security Technology Group	Snid	Miles		Manager		
Department of Commerce	National Institute of Standards and Technology (NIST)		Steinauer	Dennis		Supervisory Computer Scientist		
Department of Commerce	National Institute of Standards and Technology (NIST)	Computer Systems Laboratory					301-975-2000	
Department of Commerce	National Telecommunications and Information Administration (NTIA)	Spectrum Management Office	Gamble	Bill		Deputy Chief	202-482-1850	
Department of Commerce	National Telecommunications and Information Administration (NTIA)	NII Office					202-482-1840	
Department of Energy	Computer Incident Advisory Capability		Sparks	Sandra	L	Leader	510-422-6856	Leads a team of seven computer experts at DoE. Publishes "CIAC Notes"
Department of Energy	Energy Information Administration		Frampton	Brent		Computer Security Specialist		Quoted in Computer Digest, Jan 95 article
Department of Energy	Lawrence Livermore National Laboratory		Frank	Robert		Chief Scientist for Electronic Commerce		
Department of Health and Human Services			Faley	Pat		Acting Director, Office of Consumer Affairs		Chairs Privacy Working Group under the Information Policy Committee, IITF. Background in consumer privacy issues.
Department of Justice	Computer Crime Unit		Charney	Brian (Scott)		Unit Chief	202-514-1026	
Department of Justice	Federal Bureau of Investigation (FBI)	Criminal Justice Information Services Division -	Brewer	Ben		Chief, Programs Support		
Department of Justice	Federal Bureau of Investigation (FBI)	Electronic Crime Unit	Hendershot	Hal			202-324-6056	
Department of Justice	Federal Bureau of Investigation (FBI)	NSD/NS-5(B)	Sullivan	Johnie	A	Senior Intelligence Research Specialist	202-324-3692	
Department of Justice	Federal Bureau of Investigation (FBI)		Turney	Maureen	D	Intelligence Operations Specialist	202-324-4573	
Department of Justice	Immigration and Naturalization Service (INS)		Keys	Janet		Computer Telecommunications Security Program Manager		
Department of Justice	Justice Management Division	Computer and Telecommunications Security Staff	Edfors	Patricia	N	Director	202-616-1162	
Department of State	Bureau of Diplomatic Security	Assessment and Certification Division	Romagnoli	Jules		Chief, Assessment and Certification	202-663-0019	Quoted in Computer Digest article, Jan 95
Department of State			Miller	John				SIWS Student working on organizations and activities
Department of Transportation	United States Coast Guard		Chiswell	Ben		CAPT	202-267-1269	
Department of Transportation	United States Coast Guard		Edwards	Fred		CAPT	202-267-2576	
Department of Transportation	United States Coast Guard		Grimes	Mike	CDR			
Department of Transportation	United States Coast Guard		Inman	Mike		LCDR		
Department of Transportation			Kane	Mike		Departmental Information Systems Security Officer	202-366-9715	NIST Experience
Department of Treasury	Asst. Sec. (Mgmt/CPO) Office of Security		Ferris	Marty		Systems Security Officer	202-622-1110	

Executive Branch
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Department of Treasury	Internal Revenue Service		Robinette	Jim		Security Specialist		Quoted in Computer Digest, Jan 95 article.
Department of Treasury	Secret Service	Electronic Crimes Branch	Freihl	Bob		Chief	202-435-7700	
Department of Veterans Affairs (DVA)	Veterans Health Administration (VHA)	National Center for Information Secirity (NCIS)	Groen	Peter	J	Director		
Department of Veterans Affairs (DVA)			Boyd	Howard			202-273-5510	
Executive Office of the President	National Economic Council		Kalil	Tom			202-456-2802	
Executive Office of the President	National Security Council (NSC)		Jones	Steve		Director for Defense Policy	202-456-9191	
Executive Office of the President	Office of Management and Budget (OMB)	Office of Information and Regulatory Affairs	Katzen	Sally		Adminstrator		Chairwoman, Interagency Advisory Council, Security Standards, II Task Force
Executive Office of the President	Office of Management and Budget (OMB)	Office of Information and Regulatory Affairs	McConnell	Bruce		Chief of Information Policy	202-395-3785	Works for Sally Katzen; supports NII Security Issues Forum; Government Information Working Group; Information policy Committee.
Executive Office of the President	Office of Management and Budget (OMB)		Springer	Ed			202-395-3562	Works for McConnell
Executive Office of the President	Office of Management and Budget (OMB)		Wu	Tony		Acting Chief, Intel Branch	202-395-4800	NCS
Executive Office of the President	Office of Science and Technology (OSTP)		Fuhrman	Tom		Senior Policy Analyst	202-456-6057	Executive Office of the President; NCS
Executive Office of the President	Office of Science and Technology (OSTP)		Johnson	Lee			202-456-6060	

This page intentionally left blank.

DOEDODCID Working Group

Organization: DOEDODCID Working Group

Senior Information Warfare Official:

Information Warfare Points of Contact:

Information Warfare Related Missions and Functions:

Established in August 1993, the DOEDODCID Working Group's mission is to write the first-ever joint INFOSEC policy for the protection of information created, stored, processed, and communicated in information systems (IS) of the Director of Central Intelligence (DCI), the Secretary of Defense, and the Secretary of Energy. The joint policy will replace all existing DoD, Intelligence Community (IC), and DoE INFOSEC policy.

The DOEDODCID Working Group's legal/regulatory basis is DCID 1/16, which called for a review of the policy three years after its update in July 1988. Through networking, DoD and DoE joined the effort and current membership consists of Security Policy Board Staff (temporary chairman), CIA, DIA, DoD/OSD/DISA, NSA, NRO, FBI, NIST, State, Treasury, National Computer Security Center, DoE, Army, Navy, Air Force, and the Information Systems Secretariat/Information Systems Board.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The proposed INFOSEC policy under development by this working group will attempt to address INFOSEC in an innovative manner by encompassing the changing security and properties of data as it moves through networks, from system to system, through all of its states of transmission, processing, and storage.

Federal Agency
Computer
Security Program
Managers' Forum

Co-Chairs
S. Pitcher, DoC
E. Roback, NIST (Acting)

Organization: Federal Agency Computer Security Program Managers' Forum

Senior Information Assurance Official:

Information Assurance Points of Contact:

E. Roback, NIST

Information Assurance Related Missions and Functions:

The Federal Agency Computer Security Program Managers' Forum sponsored by NIST is a government interagency organization for advocacy and information exchange on computer security issues among Federal departments and agencies. The Federal Agency Computer Security Program Managers' Forum addresses issues related to the security of unclassified federal computer and telecommunications systems (except "Warner Amendment" systems as described in 44 U.S.C. Section 3502.)

The Managers' Forum has no legal or regulatory basis as such, but rather, was created out of need by NIST. The Managers' Forum is mainly an information-sharing body, though its charter was recently changed to make it into a more proactive group.

Membership includes the following organizations. Where a subordinate organization is indicated, both the parent and subordinate organizations are members.

- Agency for International Development
- Commodity Futures Trading Commission
- Department of Agriculture
  - Federal Crop Insurance Corporation
- Department of Agriculture
  - Agricultural Marketing Service
- Department of Commerce
  - Patent and Trademark Office
- Department of Commerce
  - National Oceanographic and Atmospheric Administration
- Department of Commerce
  - Bureau of the Census
- Department of Education
- Department of Energy
  - Federal Energy Regulatory Commission
- Department of Health & Human Services
  - Public Health Service
  - Health Care Financing Administration
  - Administration for Children & Families
- Department of Housing & Urban Development

Department of Interior
- Bureau of Land Management

Department of Justice
- Federal Bureau of Investigation
- Immigration and Naturalization Service

Department of Labor
- Employment & Training Administration
- Office of the Solicitor
- Employment Standards Administration
- Occupational Safety & Health Administration
- Office of Administrative Law Judges
- Bureau of Labor Statistics
- Pension & Welfare Benefits Administration
- Veterans Employment & Training Service

Department of State
- Bureau of Diplomatic Security

Department of Transportation
- Federal Railroad Administration
- Maritime Administration
- Federal Transit Administration
- Research & Special Programs Administration
- Federal Highway Administration
- U.S. Coast Guard
- National Highway Traffic Safety Administration
- Federal Aviation Administration

Department of Treasury

Department of Veterans Affairs
- IRM, Plan., Acq. & Security Service

Environmental Protection Agency

Equal Employment Opportunity Commission

Executive Office of the President

Farm Credit Administration

Federal Communications Commission

Federal Deposit Insurance Corporation

Federal Emergency Management Agency

Federal Maritime Commission

General Accounting Office

General Services Administration

House of Representatives
- House Information Systems

Library of Congress

National Aeronautics & Space Administration

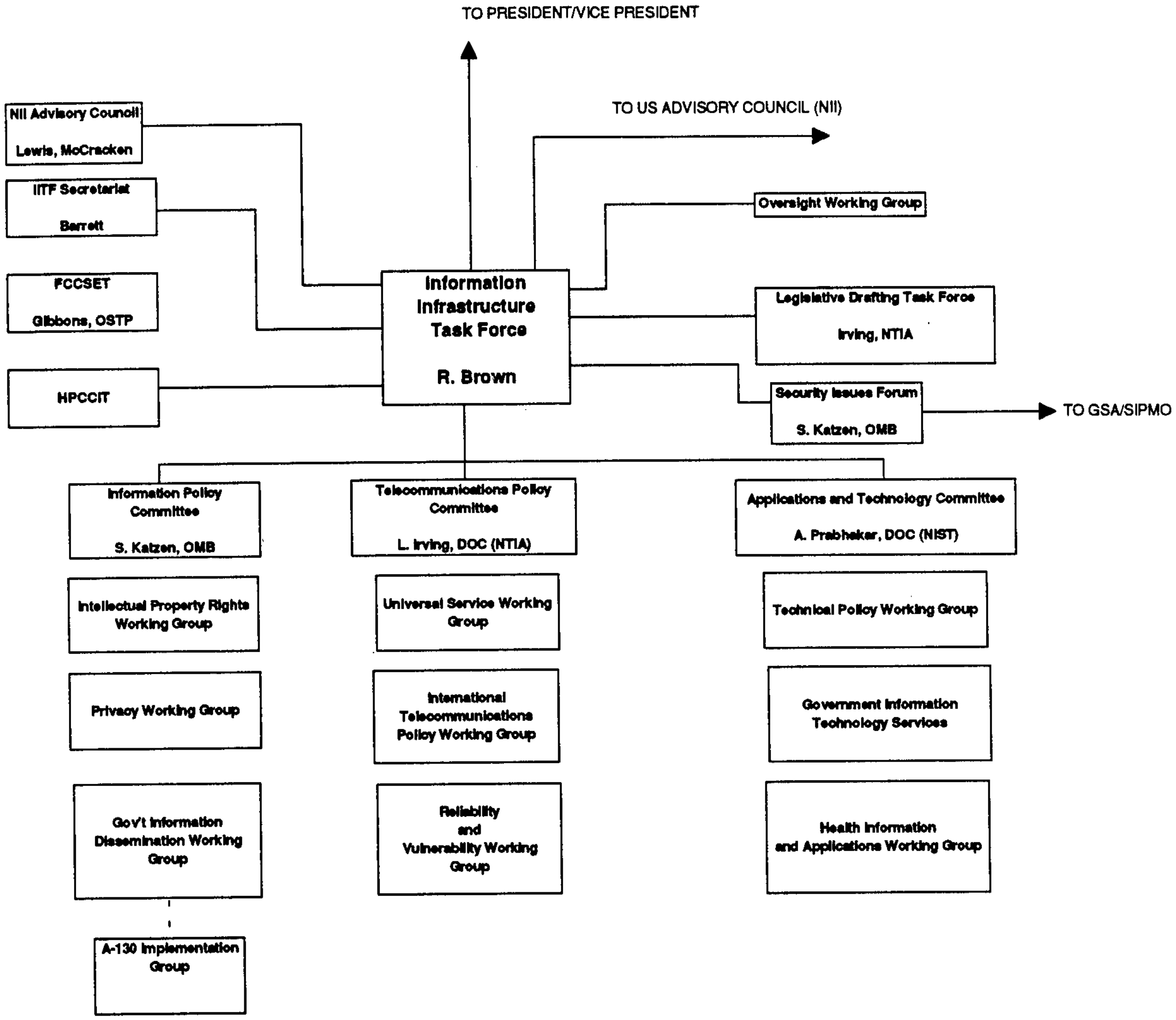
National Institute of Standards and Technology

National Labor Relations Board

National Science Foundation

National Security Agency
Nuclear Regulatory Commission
Office of Management and Budget
Office of Personnel Management
Resolution Trust Corporation
Securities and Exchange Commission
Small Business Administration
Social Security Administration
U.S. Information Agency
U.S. Senate
    Data Security Administrator
U.S. Supreme Court

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


TO PRESIDENT/VICE PRESIDENT
TO US ADVISORY COUNCIL (NII)
NII Advisory Council
Lewis, McCracken
IITF Secretariat
Barrett
FCCSET
Gibbons, OSTP
HPCCIT
Information Infrastructure Task Force
R. Brown
Oversight Working Group
Legislative Drafting Task Force
Irving, NTIA
Security Issues Forum
S. Katzen, OMB
TO GSA/SIPMO
Information Policy Committee
S. Katzen, OMB
Telecommunications Policy Committee
L. Irving, DOC (NTIA)
Applications and Technology Committee
A. Prabhakar, DOC (NIST)
Intellectual Property Rights Working Group
Privacy Working Group
Gov't Information Dissemination Working Group
A-130 Implementation Group
Universal Service Working Group
International Telecommunications Policy Working Group
Reliability and Vulnerability Working Group
Technical Policy Working Group
Government Information Technology Services
Health Information and Applications Working Group

Organization: Information Infrastructure Task Force

Senior Information Assurance Official:

Ronald H. Brown, Secretary of Commerce

Information Assurance Points of Contact:

Information Policy Committee:	Bruce McConnell
Intellectual Property Rights WG:	Edward Kazenske
Privacy Working Group:	Jerry Gates
Government Information WG:	Peter Weiss
Telecom. Policy Committee:	Tatia Williams
Universal Service Working Gp:	Tatia Williams
Rel. and Vul. Working Gp:	James Fletcher
Int. Telecom. Working Gp:	Sharon Bywater
Legislative Drafting TF:	Ellen Bloom
Committee on Appl's and Tech.:	Cita Furlani
Gov't Info. Tech. Svcs (GITS):	Jim Flyzik
Tech. Policy WG:	Howard Frank
Health Info. and Appl's WG:	John Silva
NII Security Issues Forum:	Virginia Huth
Access to IITF Bulletin Board:	202/501-1920
IITF Secretariat:	Yvette Barrett
IITF Committee Report:	Yvette Barrett

Information Assurance Related Missions and Functions:

The Clinton Administration formed the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The task force consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies.

Working together with the private sector, the participating agencies will develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of both the agencies and the country. By helping build consensus on difficult policy issues, the IITF will enable agencies to make and implement policy more quickly and effectively.

The Task Force currently is undertaking a wide-ranging examination of all issues relevant to the timely development and growth of the NII. The Administration's *Agenda for Action*, released September 15, 1993, identified nine specific principles and goals to guide government action:

1. Promoting Private Sector Investment
2. Extending the "Universal Service" Concept to Ensure that Information Resources are Available to All at Affordable Prices
3. Promoting Technological Innovation and New Applications
4. Promoting Seamless, Interactive, User-Driven Operation
5. Ensuring Information Security and Network Reliability
6. Improving Management of the Radio Frequency Spectrum
7. Protecting Intellectual Property Rights
8. Coordinating with Other Levels of Government and With Other Nations
9. Providing Access to Government Information and Improving Government Procurement

Ronald H. Brown, the Secretary of Commerce, chairs the IITF, and much of the staff work and administrative support for the task force will be done by the National Telecommunications and Information Administration (NTIA) of the Department of Commerce. The Task Force operates under the aegis of the White House Office of Science and Technology Policy and the National Economic Council. Three IITF Committees have been established: Information Policy Committee, Telecommunications Policy Committee, and a Committee on Applications and Technology.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Organization: Security Issues Forum, IITF

Senior Information Assurance Official:

Ms. Salley Katzen, Chairperson, SIF

Information Assurance Points of Contact:

Virginia Huth

Information Assurance Related Missions and Functions:

The NII Security Issues Forum will provide leadership for Federal NII security activities. It will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the Information Infrastructure Task Force (IITF) and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

The strategy of the Forum:

- The Committees of the IITF will work with the public to identify the security needs of various users of the NII.
- Forum will solicit participation from individuals, organizations, and State, local, and tribal governments.
- The Forum will also collect information concerning the impact of civil case law on security in electronic environments and will analyze the sufficiency of Federal criminal law.
- Finally, the Forum will collect and disseminate information about public and private sector security technology and management controls in order to ensure that needed security capabilities will be available.

The Forum coordinates the following IITF activities:

- Telecommunications Policy Committee (TPC), the Information Policy Committee (IPC), and the Committee on Applications and Technology (CAT).
- Intellectual Property Rights Working Group (IPRWG) and the Privacy Working Group (PWG).
- The Government Information Technology Services Working Group (GITS), will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.
- The network Reliability and Vulnerability Working Group (RVWG), with the assistance of the National Communications System and will advise the Security

Forum on (1) protection for all users from catastrophic failure of the network and the information services it provides, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks, and (2) national security and emergency preparedness requirements.

The Forum also coordinates the efforts of the following Federal Government entities:

- National Institute of Standards and Technology (NIST) will encourage the Computer System Security and Privacy Advisory Board (CSSPAB).
  NIST, will assess where research and development on security technology would be useful for the NII.
- NIST, working with other agencies, will identify Federal security products, techniques, and practices that will be useful in the NII.
- NIST will work with the Forum of Incident Response and Security Teams (FIRST) to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure a "911" capability for the NII.
- National Communications System (NCS), in coordination with the industry's National Security Telecommunications Advisory Committee (NSTAC), will work with the Network Reliability and Vulnerability Working Group to ensure that National Security and Emergency Preparedness (NS/EP) needs are accommodated in the NII.
- National Security Telecommunications and Information Systems Security Committee (NSTISSC) will identify useful security tools and techniques in the national security community that may be applicable to the NII.
- Working Group on Encryption and Telecommunications (WGET) will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps.
- The High Performance Computing and Communications (HPCC) Program will assure development and testing of new technologies for computer security suitable to a high performance environment.
- The Federal Network Council (FNC), a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Expect extensive security dialog at the national level and market forces to result in a robust National Information Infrastructure (NII). Additional departmental security requirements will have to be addressed by and budgeted for by the concerned departments.

- DoJ has prepared a comprehensive set of civil and criminal legislative proposals which will be reviewed by the Security Issues Forum (SIF). The proposals will ultimately be presented by the administration to the Congress.
- SIF has published a draft report, "NII Security: The Federal Role." The plan will be based on the series of public meetings on NII security held by the SIF. The plan will be subjected to public discussion. It will address security concerns, how to meet the concerns (market forces, private investment, government investment, etc.), legislative proposals, and a possible need for a Federal Government response and recovery plan.
- Regulatory oversight provides an opportunity to influence security in the infrastructures. While government regulatory activity is being reduced, regulation of information technology and security practices might have to increase.

Organization: Reliability and Vulnerability Working Group, IITF

Senior Information Assurance Official:

Information Assurance Points of Contact:

James Fletcher

Information Assurance Related Missions and Functions:

The RVWG has established four subgroups:

Reliability for General Users: This group is addressing issues related to overall NII reliability for Government, industry, and general users in the context of both day-to-day and emergency operations. It has identified strategies for ensuring reliability.

National Security and Emergency Preparedness: This group is addressing issues related to the NS/EP attributes the NII should support. This effort includes reviewing key industry segments such as the public switched network, cable, wireless, satellite, and broadcast and identifying features and capabilities that should be available over the NII to support NS/EP users.

Protection of the Network: This group is addressing issues related to protecting key network elements from unauthorized intrusion or manipulation and is seeking to ensure that network management information is protected. It is developing a report that will describe the potential challenges to protecting the network in the evolving NII, the threats to and vulnerabilities of the network, the resulting risks to the NII, and current efforts to reduce risks. It will conclude with an approach for addressing the system protection problem in the NII.

Integration and Planning: This group has taken inputs from each of the other subgroups and melded them into a proposed action plan that addresses reliability and vulnerability concerns. The plan describes problems, as well as key issues and necessary actions, in the areas of policy, legislation, management mechanisms, and technology. The subgroup will accomplish its objective by using an integrating framework that is currently in draft and is being addressed by the RVWG.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The RVWG has also established a working relationship with the President's National Security Telecommunications Advisory committee (NSTAC) through its NII Task Force. The RVWG subgroup leaders met with the Chairs of the NII Task Force and its three subgroup chairs to discuss issues of mutual interest and to determine how to make their efforts complementary. RVWG representatives, including the subgroup leaders, have attended meetings of the NII Task Force to continue the dialogue between the two organizations. In particular, the RVWG NS/EP subgroup has met with the NSTAC NII Task Force Architecture Subgroup and factored industry's input into its efforts to identify NII NS/EP features and capabilities.

- The RVWG determined that its overall objective was to ensure that telecommunications services and information systems of the national information infrastructure will provide: high quality service for normal operations; maximum reliability of services to meet essential public, private, and commercial needs; and capabilities that meet national security and emergency preparedness requirements. The working group agreed that the best approach to achieve that objective would be to focus on top level actions that address its span of responsibilities. The proposed Plan of Action identifies top level actions that will be pursued by the RVWG, in partnership with industry and government user groups. The plan recommends tasking for specific government agencies, recommends tasking to and from other IITF committees and working groups, and develops strategies to leverage industry and other user groups to accomplish these actions.
- The Group is developing a Reliability and Vulnerability Working Group Work Plan. The RVWG subgroups have been reviewing the proposed actions and identifying milestones to accomplish those actions. For each milestone, they are setting target dates and proposing candidate offices of primary responsibility. The RVWG plans to reach consensus on its Plan of Action. It is expected that the Plan of Action will be a "living document," capable of responding to the dynamic NII environment.

Organization: Information Management Policy Working Group

Senior Information Warfare Official:

Information Warfare Points of Contact:

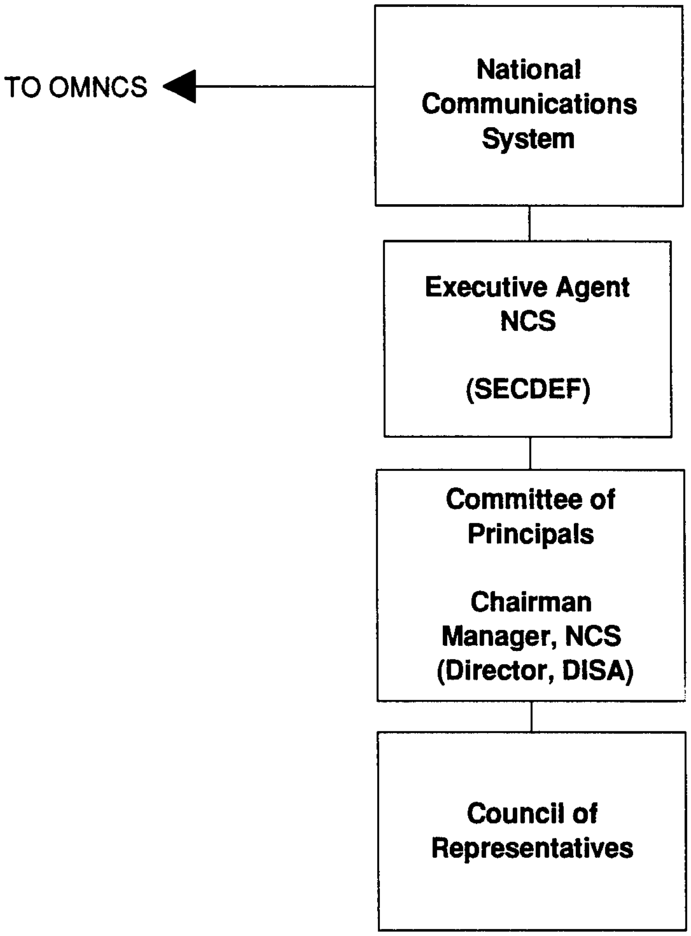
Information Warfare Related Missions and Functions:

The IMPWG is a joint DoD/DCI group created to support the Information Systems Board (ISB). Chaired by the Executive Director for Intelligence Community Affairs and the Deputy Assistant Security of Defense (Intelligence and Security), the ISB advises the DCI and the Deputy Secretary of Defense on information security matters as they pertain to interaction among organizations under their purview. The IMPWG, in turn, establishes automated intelligence information systems management and associated security policy and programs. The mission of IMPWG is to recommend top-level architectures; adopt community standards; develop policy to effect connectivity and common-user infrastructure, and interoperability; provide program and budget support; and provide liaison and coordination on security and technology issues.

Membership consists of DIA, CIA, NSA, CIO, Joint Staff, NRO, Military Services, DMA, DISA, State, Treasury, DoE, FBI, Commerce, and additional organizations as necessary. Accomplishments of the IMPWG include devising and issuing a security risk assessment methodology.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


TO OMNCS
National Communications System
Executive Agent NCS
(SECDEF)
Committee of Principals
Chairman Manager, NCS (Director, DISA)
Council of Representatives

Organization: National Communications System (NCS)

Senior Information Assurance Official:

Lieutenant General Al Edmonds, Manager, NCS

Information Assurance Points of Contact:

Mr. Fred Herr, Office of the Manager, NCS

Information Assurance Related Missions and Functions:

The Interdepartmental Committee on Communications was formed by the National Security Council on October 26, 1962, to resolve the major communications problems which had surfaced during the Cuban missile crisis. The Committee's work resulted in the creation of the NCS on August 21, 1963. The NCS was updated by Executive Order 12472, April 3, 1984, and is charged with assisting the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget in the exercise of their wartime and non-wartime emergency telecommunications functions, and their planning and oversight responsibilities. The NCS also assists in the coordination of planning for and the provision of national security and emergency preparedness telecommunications of the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. In addition, the Office of the Manager, NCS (OMNCS), provides administrative support to the President's National Security Telecommunications Advisory Committee.

Membership includes:

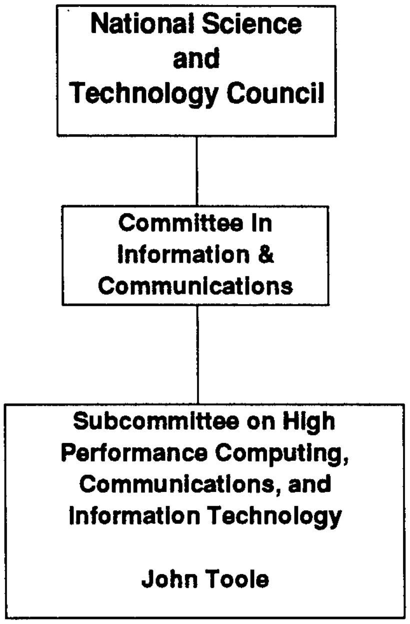
Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Justice
Department of State
Department of the Interior
Department of the Treasury
Department of Transportation
Department of Veterans Affairs
Central Intelligence Agency
Federal Communications Commission
Federal Emergency Management Agency
Federal Reserve System
General Services Administration
The Joint Staff

National Aeronautics and Space Administration
National Security Agency
National Telecommunications and Information Administration
Nuclear Regulatory Commission
United States Information Agency
United States Postal Service

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- VADM McConnell, Director, NSA, briefed the Industry Executive Subcommittee (IES) and the National Security Telecommunications Advisory Committee (NSTAC) recently on threat - really pushing NSTAC/NCS model for other industries. Director FBI also spoke to NSTAC after recent Executive Session. IES members met with CAPT Dave Henry and Mr. Dave Patterson of NSA to discuss threat. Jack Edwards briefed NSTAC response to McConnell briefing at last NSTAC meeting.
- Have briefed J33 and J6 on on-going efforts. Also briefed personnel from the Office of the Secretary of Defense (OSD) Net Assessment and Office of the Under Secretary of Defense (Policy (USD(P)).
- National Defense Infrastructures Survivability Study by USD(P) is underway. Being done by DNA as a successor to the Key Asset Protection Program (KAPP).
- NII Symposium conducted at NWC in Newport last October.
- Bellcore has 5-year contract with OMNCS to Public Switched Network (PSN) vulnerability and incident data. The data collected will build on Bellcore's Security Information Exchange data.
- SRI has produced hacker profile for OMNCS.

This page intentionally left blank.



National Science and Technology Council

Committee In Information & Communications

Subcommittee on High Performance Computing, Communications, and Information Technology

John Toole

Organization: National Science and Technology Council

Senior Information Assurance Official:

Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

President Clinton established the National Science and Technology Council (NSTC) by Executive Order 12881 on November 23, 1993. This cabinet-level council is the principal means for the President to coordinate science, space, and technology policies across the Federal government.

An important objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in areas ranging from information technologies and health research, to improving transportation systems and strengthening fundamental research. The Council prepares research and development strategies that are coordinated across Federal agencies to form an investment package that is aimed at accomplishing multiple national goals.

<u>Membership</u>
The President
The Vice President
Secretary of State
Secretary of Defense
Secretary of Interior
Secretary of Agriculture
Secretary of Commerce
Secretary of Labor
Secretary of Health and Human Services
Secretary of Transportation
Secretary of Energy
Secretary of Education
Director, Office of Management and Budget
Assistant to the President for Science and Technology
Assistant to the President for National Security Affairs
Assistant to the President for Economic Policy
Assistant to the President for Domestic Policy
Chair of the Council of Economic Advisors
Administrator, National Aeronautics and Space Administration
Administrator, Environmental Protectional Agency

Director, National Science Foundation
Director, National Institutes of Health
Director, Central Intelligence Agency
Director, Arms Control and Disarmament Agency

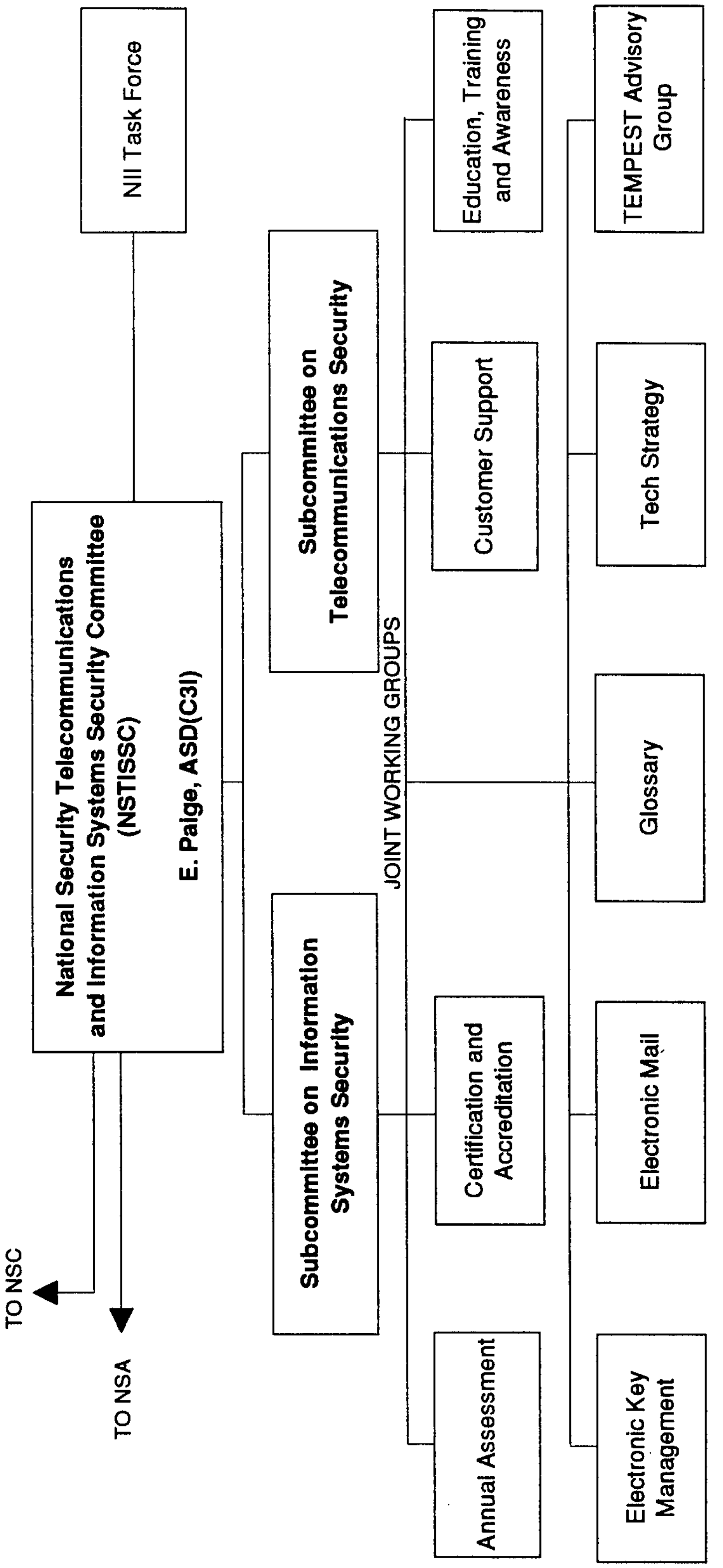
President Clinton directed the NSTC to:

- Coordinate the science and technology policy making and implementation process across Federal agencies;
- Ensure that science and technology policy decisions are consistent with the President's stated goals;
- Ensure that science and technology issues are considered in the development and implementation of Federal policies and programs;
- Further international cooperation in science and technology activities.

The Council fosters a strategic approach in determining how science and technology can help resolve complex societal needs. Today's problems demand contributions from different fields of study and a team approach from the agencies that make up the Federal R&D enterprise. The NSTC provides an interagency strategic management system to foster teamwork and enhance the ability to identify opportunities for interdisciplinary solutions.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


National Security Telecommunications and Information Systems Security Committee (NSTISSC)
E. Paige, ASD(C3I)
NII Task Force
TO NSC
TO NSA
Subcommittee on Information Systems Security
Subcommittee on Telecommunications Security
JOINT WORKING GROUPS
Annual Assessment
Certification and Accreditation
Customer Support
Education, Training and Awareness
Electronic Key Management
Electronic Mail
Glossary
Tech Strategy
TEMPEST Advisory Group

Organization: National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Senior Information Assurance Official:

Mr. E. Paige, Assistant Secretary of Defense (C3I), Chairman

Information Assurance Points of Contact:

NSTISSC Support Staff, NSA

Information Assurance Related Missions and Functions:

NSTISSC was created via NSD 42, dated 5 July 1990. NSD 42 established a senior level policy coordinating committee under the NSC, an interagency group at the operating level (NSTISSC), two subcommittees (one for information systems security and one for telecommunications security), an executive agent (DoD), and a national manager (NSA). The Policy Coordinating Committee has never met. The NSTISSC's mission was to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of the Directive.

The National Information Infrastructure (NII) Executive Committee and the NII Task Force (NIITF) were established to develop and implement a comprehensive and proactive NSTISSC program in support of the NII. The Executive Committee provides guidance and direction to the NIITF, oversee its activities, maintain liaison with NIST, as appropriate, and reports periodically to the NSTISSC on its progress. The NIITF is comprised of individuals representing NSTISSC member and observer organizations and is responsible for all NSTISSC support to the NII including:

- Facilitating liaison with various NII fora
- Coordinating the activities of NSTISSC Sub working groups in support of the NII
- Developing white papers on security issues of concern to the NII
- Providing an analysis of the common security services and requirements of member organizations
- Publishing an annual compendium of government information safeguard requirements
- Developing and implementing a campaign to increase awareness of security issues.

NSTISSC membership is categorized as follows:

- Member on the NSTISSC, STS, and SISS
- Observer on the NSTISSC, STS, and SISS
- Observer on the STS and SISS

- Observer on the STS
- Observer on the SISS
- Working Group Member

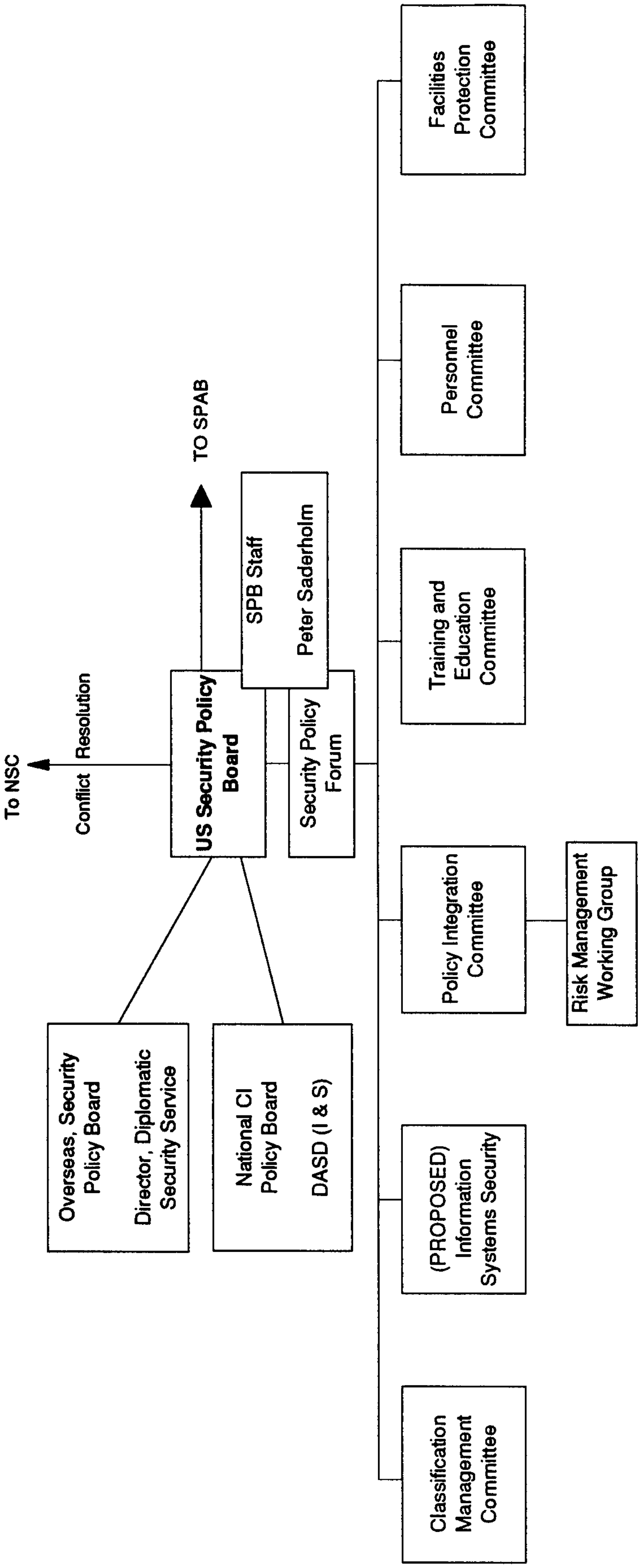
Membership in the various categories includes the following organizations. Details of which members belong to which categories can be obtained from the NSTISSC Support Staff. Where both a parent and subordinate organization are shown, both organizations participate in one or more of the above categories.

National Security Council Staff
Office of Management and Budget
U.S. Department of Agriculture
Department of Commerce
    National Institute of Standards and Technology
Department of Defense
    Joint Staff
    Army
    Navy
    Marine Corps
    Air Force
    Defense Information Systems Agency
        White House Communications Agency
    Defense Intelligence Agency
    Defense Investigative Service
    Defense Logistics Agency
    Defense Mapping Agency
    Defense Nuclear Agency
    National Security Agency
Department of Education
Department of Energy
Department of Health and Human Services
    Indian Health Service
    Public Health Service
Department of Housing and Urban Development
Department of the Interior
Department of Justice
    Drug Enforcement Administration
    Federal Bureau of Investigation
    Immigration and Naturalization Service
Department of Labor
Department of State
Department of Transportation
    Federal Aviation Administration
    U.S. Coast Guard

Department of the Treasury
U.S. Customs Service
U.S. Secret Service
Department of Veterans Affairs
Director of Central Intelligence/Central Intelligence Agency
Federal Communications Commission
Federal Emergency Management Agency
Federal Reserve System
General Services Administration
National Aeronautics and Space Administration
National Communications System
Nuclear Regulatory Commission
Office of Personnel Management
Securities Exchange Commission
U.S. Information Agency

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

NSTISSC accomplishments to date include the development of policies, guidelines, instructions, and standards; provided systems security guidance; produced the annual assessment of the "health" of national security systems; provided release approval to foreign governments and international organizations; maintained the national issuance system; and produced special publications.


To NSC
Conflict Resolution
US Security Policy Board
TO SPAB
SPB Staff
Peter Saderholm
Security Policy Forum
Overseas, Security Policy Board
Director, Diplomatic Security Service
National CI Policy Board
DASD (I & S)
Classification Management Committee
(PROPOSED) Information Systems Security
Policy Integration Committee
Risk Management Working Group
Training and Education Committee
Personnel Committee
Facilities Protection Committee

Organization: United States Security Policy Board (USSPB)

Senior Information Assurance Official:

Peter Saderholm, Director, USSPB Staff

Information Assurance Points of Contact:

Vickie LaBarre, USSPB Staff

Information Assurance Related Missions and Functions:

The Secretary of Defense (SECDEF) and the Director of Central Intelligence (DCI) created the Joint Security Commission (Commission) in May 1993 to review the security practices and procedures under their authorities.

The Commission concluded that the problems of fragmentation and inconsistency in security policy development, implementation, and oversight must be resolved in order to make meaningful improvements in the overall effectiveness of US Government security. The commission proposed the creation of a unifying structure to "provide leadership, focus, and direction to the government security communities."

Under PDD-29, the U.S. Security Policy Board becomes the umbrella under which all the elements of security are organized. It is responsible for not only what to protect (classification management) but also how to protect it (security countermeasures). The Board receives overall policy guidance from the NSC and accepts responsibility for the flow of policy direction both to and from the NSC. Consistent with PDD-29, the Board is assisted by the Security Policy Advisory Board (Advisory Board), the Security Policy Forum (Forum), and various intergovernmental committees and working groups.

Committees and ad hoc working groups organized along security discipline lines support the Forum. The principle committees proposed to support the Board structure include:

- A Personal Security Committee (PSC) to address all personnel security policies, procedures, and practices applicable to US Government departments and agencies;

- A Facilities Protection Committee (FPC) to address all policies, practices and procedures applicable to the protection of US Government and industrial facilities; physical, technical, and TEMPEST;

- An Information Systems Security Committee (ISSC) charged with coupling the development of policy for both the classified and the sensitive but unclassified communities;

- A Classification Management Committee (CMC) charged with the development of classification management policy within the context of the overall security policy framework;

- A Training and Professional Development Committee (TPDC) to standardize and coordinate security training, education, and awareness and to achieve efficiencies in the development and delivery of such training, and;

- A Policy Integration Committee (PIC) charged to ensure overarching themes are integrated into all U.S. Government security policy and encourage synergy in the activities of the other standing committees.

As of 1 June 1995, all committees have been established except the Information Systems Security Committee.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The end of the Cold War has dramatically changed the threats that defined the security policies and procedures for protecting our government's information, facilities and people. While some threats have been reduced, others have remained relatively stable or have increased. Our understanding of the range of issues that affect our national security continues to evolve. Economic issues are of increasing concern and are competing with traditional political and military issues for resources and attention. Technologies, such as those used to create weapons of mass destruction are evolving and proliferating. With this greater diversity of threats, there is wide recognition that the security policies, practices, and procedures developed during the Cold War must be reexamined and changed. We require a new security process based on sound threat analysis and risk management practices. A process which can adapt our security policies, practices and procedures as the economic, political and military challenges to our national interests continue to evolve.
- The Director of Central Intelligence and Secretary of Defense's Joint Security Commission identified four principles which should guide the formulation, evaluation and oversight of our security policy:
    - * Our security policies and services must realistically match the threats we face and must be sufficiently flexible to facilitate change as the threats evolve.
    - * Our security policies and practices must be consistent and enable us to allocate scarce resources effectively.
    - * Our security standards and procedures must result in the fair and equitable treatment of all Americans upon whom we rely to guard our nation's security.
    - * Our security policies, practices and procedures must provide the security we need at a price we can afford.
- The National Security Act of 1947, as amended, specifies that is the duty of the National Security Council (NSC) to consider policies on matters of common interest to the

departments and agencies of the Government concerned with the national security and to make recommendations to the president in connection therewith. Consistent with the National Security Act of 1947, the President has directed the establishment of a new security policy structure, under the direction of the NSC, for the coordination, formulation, evaluation and oversight of security policy guided by the above principles.

- Nothing in this directive amends or changes the authorities and responsibilities of the members of the Policy Board, including, Director of Central Intelligence (DCI), Secretary of Defense, Secretary of State, Secretary of Energy, Secretary of Commerce, Attorney General, Director of the FBI, Chairman of the Nuclear Regulatory Commission, or Director of the Information Security Oversight Office as contained in the National Security Act of 1947, other existing laws or Executive Orders.
- The President directed the following:
    * The Joint Security Executive Committee established by the Deputy Secretary of Defense and the Director of Central Intelligence is designated the Security Policy Board and directed to report to the President through the Assistant to the President for National Security Affairs. The existing national security countermeasures policy and coordination structure, the National Advisory Group for Security Countermeasures, is hereby abolished and its functions transferred to the Security Policy Board.
    * The Security Policy Board will consist of the Director of Central Intelligence, the Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs of Staff, the Deputy Secretary of State, the Under Secretary of Energy, the Deputy Secretary of Commerce, the Deputy Attorney General, one Deputy Secretary from another non-defense related agency and one representative from the Office of Management and Budget and the NSC staff. The additional non-defense agency representative will be rotated on an annual basis and selected by the non-defense agency members of the Security Policy Forum established below. Senior representatives of other Departments and Agencies will be invited members at such times as the Security Policy Board considers security issues germane to their responsibilities.
    * The Chairman of the Security Policy Board will be designated by the Assistant to the President for National Security Affairs on behalf of the President.
    * The Security Policy Board will consider, coordinate and recommend for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices. The Security Policy Board will be the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State. This Board will coordinate the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements. In coordinating security policy, procedures and practices, the Policy Board will ensure that all U.S. Departments and Agencies affected by such decisions are allowed to comment on such proposals.

* Policy disputes that cannot be resolved by this Board will be forwarded to the Principals Committee of the National Security Council.
* A Security Policy Advisory board was established to serve as an independent and non-governmental advisory body on U.S. security policy. Five members, including a Chairman, will be appointed by the President for terms of up to three years. The Chairman will report annually to the President through the Assistant to the President for National Security Affairs on implementation of the four policy principles identified above. The Security Policy Advisory Board will also provide a non-governmental and public interest perspective on security policy initiatives to the Security Policy Board and the intelligence community.
* The Security Policy Forum established under the Joint Security Executive Committee is retained under the Security Policy board to consider security policy issues raised by its members or any other means; develop security policy initiatives and obtain Department and Agency comments on these initiatives for the Policy Board; evaluate the effectiveness of security policies; monitor and guide the implementation of security policy to ensure coherence and consistency; and oversee the application of security policies to ensure that they are equitable and consistent with national goals. Policy Forum membership will include one senior representative from the Office of Secretary of Defense, Joint Chiefs of Staff, each Military Department, including the U.S. Coast Guard, Defense Intelligence Agency, National Security Agency, Central Intelligence Agency, Commerce, Energy, Justice, State, Treasury, Transportation, Federal Bureau of Investigation, National Reconnaissance Office, Federal Emergency Management Agency, General Services Administration, Defense Information Systems Agency/National Communications System, Office of personnel Management, Information Security Oversight Office, Nuclear Regulatory Commission, NASA, Office of Management and Budget, and other agencies representatives as invited by the Security Policy Board Chairman.
* The Security Policy Board and Forum may establish interagency working groups as necessary to carry out their functions and ensure interagency input and coordination of security policy, procedures and practices.
* The existing Department of State Overseas Security Policy Group is hereby designated as, and its functions transferred to, the Overseas Security Policy Board and directed to report to the president through the Assistant to the President for National Security Affairs. The Overseas Security Policy Board will be chaired by the Director of the Diplomatic Security Service and its membership will consist of representatives from the Department of State, Agency for International Development, CIA, Defense Intelligence Agency, FBI, Commerce, Justice, Treasury, Transportation, National Security Agency, United States Information Agency, Peace Corps, Federal Aviation Administration, Foreign Agricultural Service and the DCI's Center for Security Evaluation, Office of Management and Budget, NASA, Arms Control and Disarmament Agency.
* The Overseas Security Policy Board will consider, develop, coordinate and promote policies, standards and agreements on overseas security operations,

programs and projects which affect all U.S. Government agencies under the authority of a chief of mission abroad.

- The National Counterintelligence Policy Board established by PDD-24, the Security Policy Board and the Overseas Security Policy Board, will coordinate as necessary on policy issues that may be of mutual concern and each Board will implement procedures for such coordination. Conflicts between these Boards that cannot be resolved will be referred to the Principals Committee of the National Security Council. The Chairman of these Boards will meet at least on an annual basis to review policy coordination.
- The Security Policy Board, Forum, and any interagency working groups established by these bodies will be supported by a Staff which will operate under the direction of the Security Policy Board. This Staff will also provide administrative and personnel support to the Security Policy Advisory Board which will operate independent of other Staff functions and personnel under the direction of the Chairman of this Advisory Board. Staff personnel will be provided or funded by the member agencies of the Security Policy Board.

This page intentionally left blank.

Interagency Group
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Department of Commerce	National Institute of Standards and Technology (NIST)		Roback	Ed			301-975-3696	
Department of Commerce			Brown	Ron		Secretary of Commerce		
Department of Defense	National Security Agency (NSA)	NSTISSC Support Staff					301-688-7355	
Information Infrastructure Task Force	Commmittee on Applications and Technology		Furlani	Cita			301-975-4529	
Information Infrastructure Task Force	Government Information Technolog Services		Flyzik	Jim			202-622-1592	
Information Infrastructure Task Force	Government Information Working Group		Weiss	Peter			202-395-3785	
Information Infrastructure Task Force	Health Information and Applications Working Group		Silva	John			703-696-2221	
Information Infrastructure Task Force	IITF Secretariat		Barrett	Yvette			202-482-1835	
Information Infrastructure Task Force	Information Policy Working Group		McConnell	Bruce			202-395-3785	
Information Infrastructure Task Force	Int. Telecom Working Group		Bywater	Sharon			202-482-1304	
Information Infrastructure Task Force	Intellectual Property Rights Working Group		Kazenske	Edward			703-305-8600	
Information Infrastructure Task Force	Legislativew Drafting Task Force		Bloom	Ellen			202-482-1551	
Information Infrastructure Task Force	NII Security Forum		Huth	Virginia			202-395-3785	Works for Sally Katzen
Information Infrastructure Task Force	Privacy Working Group		Gates	Jerry			301-457-2515	
Information Infrastructure Task Force	Security Issues Forum		Katzen	Sally				
Information Infrastructure Task Force	Technology Policy Working Group		Frank	Howard			703-696-2409	
Information Infrastructure Task Force	Universal Service Working Group		Williams	Tatia			202-482-1551	
National Communications System	Office of the Manager or the National Communications System (OMNCS)	Joint Secretariat	Fletcher	Jim		LTC, USA	703-607-6207	Supports the NII Reliability and Vulnerability Working Group and associated subgroups.
National Communications System	Office of the Manager or the National Communications System (OMNCS)		Herr	Fred			703-607-6184	
National Communications System			Edmonds	Al				
National Security Telecommunications and Information Systems Security Committee			Paige	Emmett		ASD(C3I)		
U.S. Security Policy Board	SPB Staff		Saderholm	Peter		Director	703-602-6997	ACCE Panel Presentation
U.S. Security Policy Board			LaBarre	Vicki			703-602-7065	Security Policy

This page intentionally left blank.

This page intentionally left blank.

Committee of Advisors on Science and Technology

Organization: Committee of Advisors on Science and Technology

Senior Information Assurance Official:

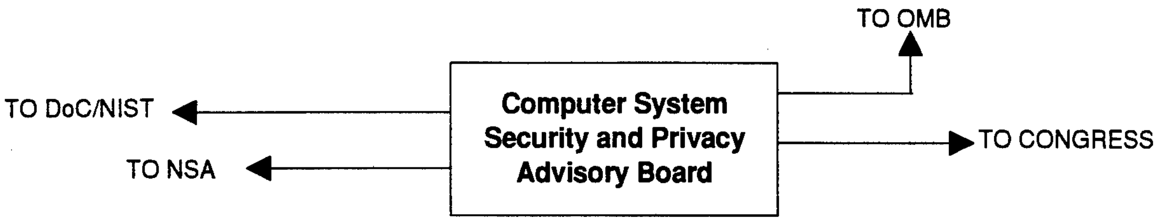
Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

President Clinton established the President's Committee of Advisors on Science and Technology (PCAST) by Executive Order 12882 at the same time that he established the NSTC. The PCAST serves as the highest level private sector advisory group for the President and for the NSTC. The Committee members are distinguished individuals appointed by the President, and are drawn from industry, education and research institutions, and other nongovernmental organizations. The Assistant to the President for Science and Technology co-chair the Committee with a private sector member selected by the President.

The formal link between the PCAST and the NSTC ensures that national needs remain an overarching guide for the NSTC. The PCAST provides feedback about Federal programs and actively advises the NSTC about science and technology issues of national importance.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


TO OMB
TO DoC/NIST
Computer System Security and Privacy Advisory Board
TO CONGRESS
TO NSA

Organization: Computer System Security and Privacy Advisory Board

Senior Information Assurance Official:

Dr. Willis Ware, Chairman, RAND Corporation

Information Assurance Points of Contact:

E. Roback, NIST

Information Assurance Related Missions and Functions:

In accordance with the requirements of Section 3 of the Computer Security Act of 1987 (P.L. 100-235), the Secretary of Commerce established the Computer System Security and Privacy Advisory Board, pursuant to the Federal Advisory Committee Act.

The Computer Security Act specifies that the Board's mission is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

The Board examines those issues affecting the security and privacy of sensitive unclassified information in federal computer and telecommunications systems. The Board's authority does not extend to private-sector systems or federal systems which process classified information.

The Board advises the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) on computer security and privacy issues pertaining to sensitive unclassified federal computer systems. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and appropriate committees of Congress.

NIST personnel serve as the Board's Secretariat. Other federal agency personnel may also assist the Board's activities as specified in the Computer Security Act of 1987.

The membership of the board includes: four members outside the Federal Government eminent in the computer or telecommunications industry, including at least one representative of small or medium sized companies in such industries; four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed or representatives of a producer of computer or telecommunications equipment; and four members from the Federal Government, including one from the National Security Agency, who have computer systems management experience, including experience in computer systems security and privacy.

The Board reports through the Director of the National Institute of Standards and Technology to the Secretary of Commerce, and as required by Section 3 of the Computer Security Act of 1987, to the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. Members include:

Dr. Willis Ware (Chairman)
Computer Research Staff
RAND

Ms. Genevieve M. Burns
Consultant

Mr. Gaetano Gangemi
Wang Laboratories, Inc.

Mr. Stephen A. Trodden, Inspector General
Department of Veterans Affairs

Mr. Charlie Baggett, Jr.
National Security Agency

Mr. Chris Castro
KPMG Peat Marwick

Ms. Sandra Lambert
Citibank

Mr. Randolph Sanovic
Mobil Corporation

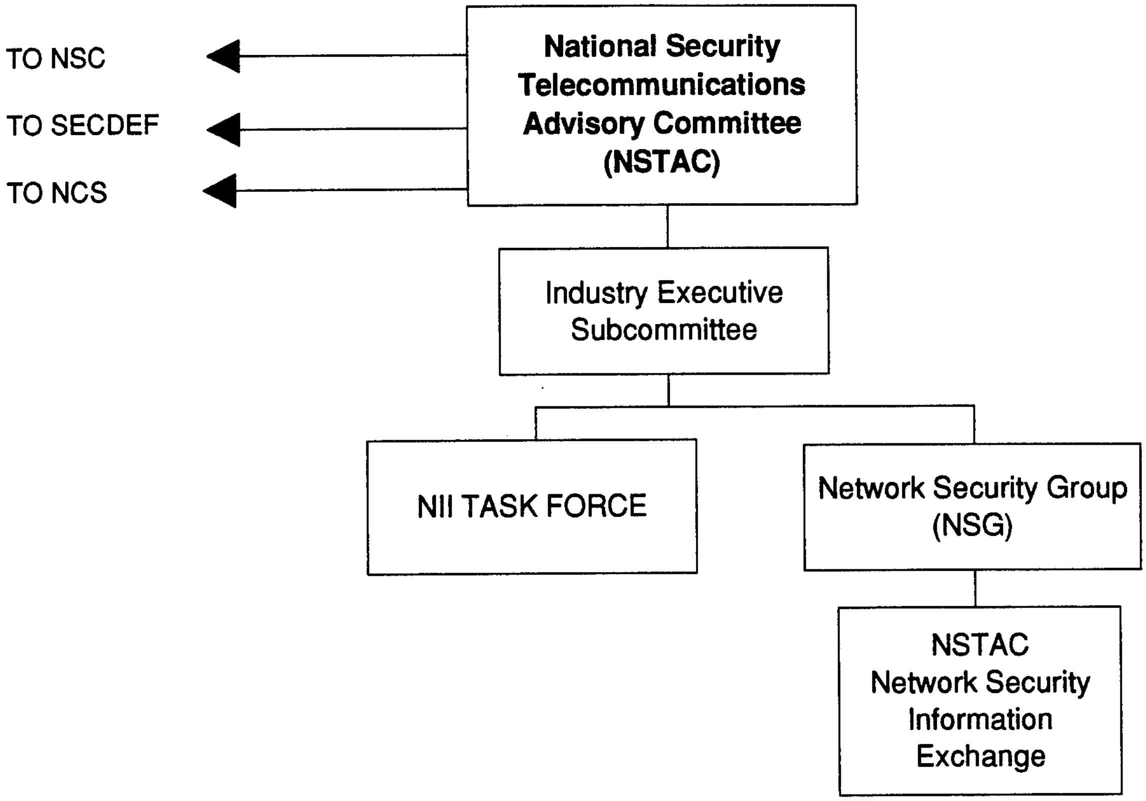
Ms. Linda Vetter
Senior President, R&D
Walker Interactive Systems
Technology Division
Oracle

Mr. Stephen T. Walker, President
Trusted Information Systems, Inc.

Mr. Bill Whitehurst
Director of Data Security Programs
International Business Machines Corporation

Mr. Joe Leo
Deputy Administrator for Management
Food and Consumer Service
USDA

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


TO NSC
TO SECDEF
TO NCS
National Security Telecommunications Advisory Committee (NSTAC)
Industry Executive Subcommittee
NII TASK FORCE
Network Security Group (NSG)
NSTAC Network Security Information Exchange

Organization: National Security Telecommunications Advisory Committee

Senior Information Assurance Official:

Bob Carpenter, TRW, Information Assurance Task Force
Bruce Roberts, UNISYS, Information Assurance Task Force
Carl Ripa, Bellcore, NII Task Force
Amy Copeland, CSC, NII Task Force
Bob Donahue, EDS, NII Task Force

Information Assurance Points of Contact:

Mr. Fred Herr, Office of the Manager, National Communications Systems

Information Assurance Related Missions and Functions:

E.O. 12382 established the President's National Security Telecommunications Advisory Committee (NSTAC) to provide advice and information from the perspective of industry to the President and the Executive Branch with respect to national security telecommunications policy and enhancements to NS/EP telecommunications.

Current NSTAC members are:

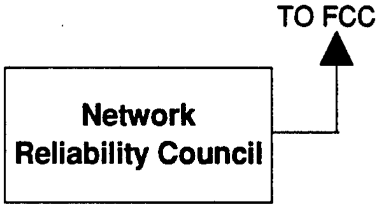
AT&T Corporation
Bank of America
Bell Communications Research, Incorporated
The Boeing Company
Communications Satellite Corporation
Computer Sciences Corporation
Electronic Data Systems
GTE Corporation
Harris Corporation
Hughes Aircraft Company
International Business Machines Corporation
Interdigital
ITT Corporation
Lockheed-Martin
Loral Corporation
MCI Communications Corporation
MFS Communications Company, Inc.
Motorola, Incorporated
Northern Telecom, Incorporated
Pacific Telecom, Incorporated
Rockwell International Corporation
Sprint Corporation

TRW, Incorporated
Unisys Corporation
U.S. Telephone Association
U.S. West, Incorporated
Williams Telecommunications Group, Incorporated

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- At the 15th meeting of the NSTAC on May 27, 1993, Dr. John Gibbons, Director, OSTP, stated that the federal government would be looking to the NSTAC for advice on how the emerging NII and its dual-use applications could meet critical NS/EP requirements currently managed by the Defense Information Systems Administration and the NCS. In response, the NSTAC established its NII Task Force (NII TF), an industry-led group analyzing the NS/EP dimensions of the NII.
- NSTAC has also recently established an information assurance task force.
- Many activities of the NSTAC's subordinate groups result in technical reports, recommendations to the President, and operational programs. For example, the National Coordinating Center for Telecommunications (NCC), a joint industry-government operations center for day-to-day planning, coordination, and exercise of NS/EP telecommunications, is the direct result of an NSTAC recommendation. Also, the Telecommunications Service Priority (TSP) System and the National Telecommunications Management Structure (NTMS), once NSTAC issues, are now operational programs. Much of the Government's National Level Program (NLP) for survivable and robust NS/EP telecommunications is a result of the President's NSTAC actions and recommendations.
- Separate industry and Government Network Security Information Exchange (NSIE) groups have been created and meet regularly to counter the threat of hackers and software disturbances to the PSN.
- A network security symposium was held in February 1994, and was considered a great success by both industry and Government attendees.
- The NSTAC's NII Task Force addressed a broad based agenda through three subgroups: (1) Applications, (2) Policy, and (3) Future Commercial Systems and Architecture.
- An NII Symposium, held in October 1994, was a collaborative forum in which senior Government and industry executives candidly discussed key NS/EP issues related to the NII.

This page intentionally left blank.


TO FCC
Network
Reliability Council

Organization: Network Reliability Council, FCC

Senior Information Assurance Official:

Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The Network Reliability Council (NRC), an organization of CEOs from leading telecommunications carriers, manufacturers and user communities, was created in the spring of 1992 by the FCC to investigate the reliability of the public switched network following a series of service outages in 1991. The efforts of the Council culminated in a one thousand plus page document, "Network Reliability: A Report to the Nation." The Council presented the report in fulfillment of its original charter and mission. To ensure that a broadly-based committee of industry experts remained actively involved in reliability and Network Outage matters, the Council established the Network Reliability Steering Committee (NRSC) within the Alliance for Telecommunications Industry Solutions (ATIS). The Council established the NRSC to track and analyze outages reported to the FCC and issue quarterly, and annual reports to the Commission and the industry.

In July 1994, the FCC revamped and expanded the Network Reliability Council (NRC), gave it a new charter and extended its assignment until January, 1996. The revised charter calls on the Council to: 1) evaluate the reliability of network services in the United States on a local and regional basis; 2) evaluate potential new risks from new interconnection arrangements; 3) access the impact of changing technologies including cable television and wireless technologies; 4) evaluate access to emergency services during network outages; and 5) determine whether network outages have disproportionate impact on certain geographic areas or certain demographic groups. The OMNCS is represented on the Council's steering committee which will work these issues. The steering committee is called "NO REST II." This is a follow-on to the original <u>N</u>etw<u>o</u>rk <u>R</u>eliability <u>S</u>teering <u>T</u>eam (NO REST).

Members of the NRC include:

<u>Interexchange Carriers</u>

AT&T
MCI Comm. Corp.
Sprint

Local Exchange Carriers
Ameritech
Bell Atlantic
Bell South
GTE Corporation
NYNEX Corporation
Pacific Telesis
Southwestern Bell
US West, Inc.
Rochester Telephone

Research and Standards Groups
Bell Communications Research (Bellcore)
Alliance for Telecommunications Industry Solutions (ATIS)
Cox Cable Communications, Inc. (Cable Labs)

Trade Associations
Association for Local Telecommunications Services (ALTS)
Competitive Telecommunications Association (COMPTEL)
Organization for the Protection and Advancement of Small Telephone Companies (PASTCO)
United States Telephone Association (USTA)
Telecommunications Industry Association (TIA)
National Cable Television Association (NCTA)
Cable Telecommunications Association (CATA)
Personal Communications Industry Association (PCIA)
Cellular Telecommunications Industry Association (CTIA)

Large Consumer Representatives
Ad Hoc Telecommunications Users Group
International Communications Association (ICA)

Small Consumer Representatives
Alliance for Public Technology
National Association of State Utilities Consumer Advocates (NASUCA)

Cable Companies
Time Warner Communications

Satellite Representatives
Hughes Space and Communications Company

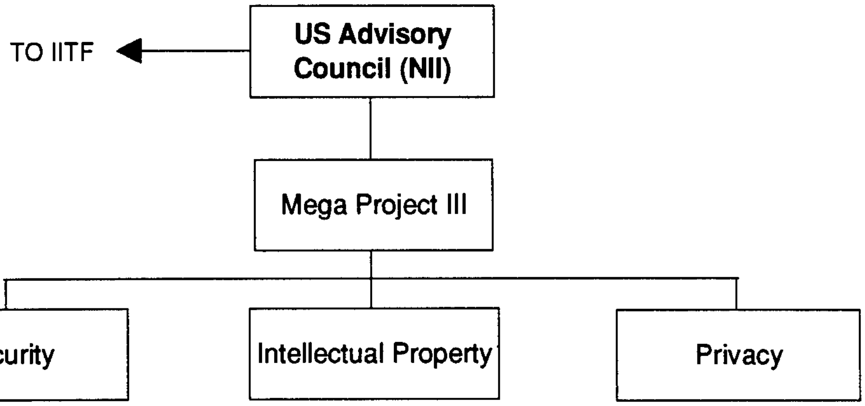
Government Related Organizations
National Association of Regulatory Utility Commissioners (NARUC)
National Communications System

Labor
Communications Workers of America, AFL-CIO

Computer Firms
IBM

Observer Members
National Telecommunications and Information Administration, U.S. Department of Commerce
Office of Science and Technology Policy, White House

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


TO IITF
US Advisory Council (NII)
Mega Project III
Security
Intellectual Property
Privacy

Organization: U.S. Advisory Council (National Information Infrastructure)

Senior Information Assurance Official:

Information Assurance Points of Contact:

Yvette Barrett, IITF Secretariat

Information Assurance Related Missions and Functions:

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Through Executive Order No. 12864. the President established an Advisory Council on the National Information Infrastructure. The Council is identifying appropriate government action within these guidelines to advise the Secretary of Commerce, Ronald H. Brown, on matters related to the development of the NII. Secretary Brown originally appointed 37 members to serve a two-year term on the Advisory Council. The Council members represent the many different stakeholders in the NII, including industry, labor, academic, public interest groups, and state and local governments.

Current members are:

Mr. Morton Bahr, President
Communications Workers of America, AFL-CIO
Dr. Toni Carbo Bearman, Dean and Professor,
School of Library and Information Science University of Pittsburgh
Ms. Marilyn Bergman
President, American Society of Composers, Authors, and Publishers (ASCAP)
Ms. Bonnie Laverne Bracey, Teacher
Ashlawn Elementary School, Arlington, Virginia
Mr. John F. Cooke, President
The Disney Channel
Ms. Esther Dyson, President
EDventure Holdings
Mr. William C. Ferguson, Chairman and Chief Executive Officer
NYNEX corporation
Dr. Craig Fields, Chairman and Chief Executive Officer
Microelectronics and Computer Technology Corporation
Mr. Jack Fishman, Publisher
Citizen-Tribune

Ms. Lynn Forester, President and Chief Executive Officer
  Firstmark Holdings, Inc.
Honorable Carol Fukunaga, Senator
  State of Hawaii
Mr. Jack Golodner, President
  Department for Professional Employees, AFL-CIO
Mr. Eduardo Gomez, President and General Manager
  KABQ Radio, Albuquerque, New Mexico
Mr. Haynes G. Griffin, President and Chief Executive Officer
  Vanguard Cellular Systems, Inc.
Dr. George Heilmeier, President and Chief Executive Officer
  Bellcore (Bell Communications Research)
Ms. LaDonna Harris, President
  Americans for Indian Opportunity
Ms. Susan Herman, General Manager
  Department of Telecommunications, City of Los Angeles
Mr. James R. Houghton, Chairman and Chief Executive Officer
  Coming Incorporated
Mr. Stanley S. Hubbard, Chairman and Chief Executive Officer
  Hubbard Broadcasting, Inc. and the United States Satellite Broadcasting Company, Inc.
Mr. Robert L. Johnson, Founder and President
  Black Entertainment Television (BET)
Dr. Robert E. Kahn, President
  Corporation for National Research Initiatives (CNRI)
Ms. Deborah Kaplan, Vice President
  World Institute on Disability
Mr. Mitchell Kapor, Chairman
  Electronic Frontier Foundation
Mr. Delano E. Lewis, President and Chief Executive Officer
  National Public Radio (NPR)
Mr. Alex J. Mandl, Chief Executive Officer
  Communications Services Group, AT&T
Mr. Edward R. McCracken, Chairman and Chief Executive Officer
  Silicon Graphics, Inc.
Dr. Nathan Myhrvold, Senior Vice President of Advanced Technology
  Microsoft Corporation
Mr. N.M. (Mac) Norton, Jr., Attorney-at-Law
  Wright, Lindsey & Jennings
Mr. Vance K. Opperman, President
  West Publishing Company
Ms. Jane Smith Patterson, Advisor to the Governor of North Carolina
  for Policy, Budget and Technology
Ms. Frances W. Preston, President and Chief Executive Officer
  Broadcast Music Incorporated (BMI)

Mr. Bert C. Roberts, Jr., Chairman and Chief Executive Officer
MCI Communications Corporation
Mr. John Sculley, Former Chairman
Apple Computers, Inc.
Ms. Joan H. Smith, Chairman
Oregon Public Utility Commission
Mr. Al Teller, Chairman and Chief Executive Officer,
MCA Music Entertainment Group
Mr. Lawrence Tisch, President and
Chief Executive Officer, CBS, Incorporated
Mr. Jack Valenti, Chief Executive Officer and President
Motion Picture Association of America

This page intentionally left blank.

Advisory Committee
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
NIST			Roback	Ed			301/975-3696	CSSPAB
Office of the Manager or the National Communications System (OMNCS)			Herr	Fred			703/607-6184	NSTAC support
RAND	Corporate Research Staff		Ware	Willis			310/393-0411	CSSPAB
U. S. Advisory Council (NII)	IITF Secretariat		Barrett	Yvette			202-482-1835	
U. S. Advisory Council (NII)			Lewis	Delano		Co-Chair	202-414-2000	CEO, National Public Radio
U. S. Advisory Council (NII)			McCracken	Ed		Co-Chair	310-312-0227	Chairman, Silicon Graphics

This page intentionally left blank.

This page intentionally left blank.

Central Intelligence Agency

J. Deutch

Organization: Central Intelligence Agency

Senior Information Warfare Official:

John Deutch, Director of Central Intelligence
RADM Dennis Blair, Deputy for Military Issues

Information Warfare Points of Contact:

Larry Gershwin, National Intelligence Council, National Intelligence Officer:
Strategic Forces
Sue Gordon, Office of Science & Weapons Research, Critical Technologies Branch
Frank Watanabe, Development Capabilities Division
Mark Zimmerman, Development Capabilities Division
Jasper Welch, Military Applications Panel

Information Warfare Related Missions and Functions:

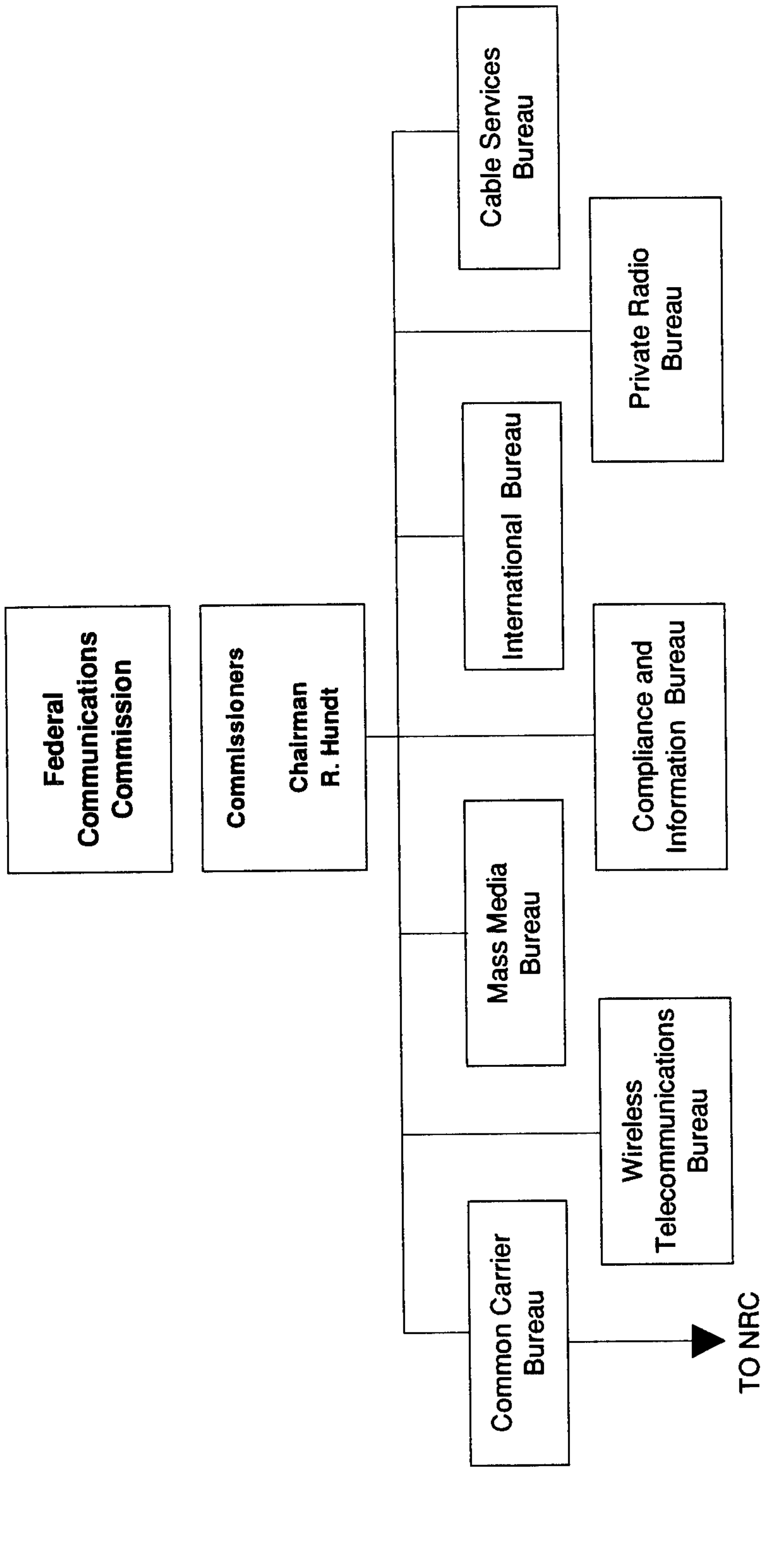
Overall policy and tasking for the Intelligence Community in general, and for the CIA in particular to supply foreign intelligence support to the U.S. government on information warfare issues and activities. CIA is the National Intelligence Council responsible for national intelligence estimates. Larry Gershwin has been the NIO charged with this responsibility. He has completed an Intelligence Community Assessment on information warfare earlier this year, and is engaged in drafting a National Intelligence Estimate on IW; currently estimated to be completed in January 1996.

The Office of Science and Weapons Research (OSWR) focuses on scientific and technical intelligence on foreign military R&D and system development and acquisition. The Critical Technologies Division has been tasked with looking at new technology development and related acquisition programs for information system technologies, inter alia.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- This is a relatively new thrust for the Intelligence Community, and they have just begun to adjust to deal with this "new" warfare area.
- The DCI has a Military Applications Panel, chaired by Jasper Welch (MGen, USAF, Ret.) which has an IW subpanel, chaired by Glen Otis (GEN, USA, Ret. and former CINCUSAREUR).

This page intentionally left blank.


Federal Communications Commission
Commissioners
Chairman R. Hundt
Common Carrier Bureau
Wireless Telecommunications Bureau
Mass Media Bureau
Compliance and Information Bureau
International Bureau
Private Radio Bureau
Cable Services Bureau
TO NRC

Organization: Federal Communications Commission (FCC)

Senior Information Assurance Official:

Andrew Barrett, Defense Commissioner

Information Assurance Points of Contact:

Arlan Van Doorr, Deputy Bureau Chief, Compliance and Information Bureau,
Representative to the NCS Committee of Principals
Roy Kolly, Compliance and Information Bureau, Representative to the
NCS Committee of Representatives
Herb Neumann, FCC Representative to the National Coordination Center

Information Assurance Related Missions and Functions:

The Federal Communications Commission regulates interstate and foreign communications by radio, television, wire, and cable. It is responsible for the orderly development and operation of broadcast services and the provision of rapid, efficient nationwide and worldwide telephone and telegraph services at reasonable rates. This also includes the promotion of safety of life and property through radio and the use of radio and television facilities to strengthen the national defense. Recent reorganization of the FCC reflects evolution of the FCC in concert with industry evolution.

The Commission uses a variety of measures to track telephone company service performance including customer satisfaction levels, dial tone response, transmission quality and call failures due to network capacity or equipment problems. In response to several telecommunications outages in the early 1990's, the FCC established outage reporting requirements and established a federal advisory committee, the Network Reliability Council (NRC). An organizational summary of the NRC can be found under Advisory Committees.

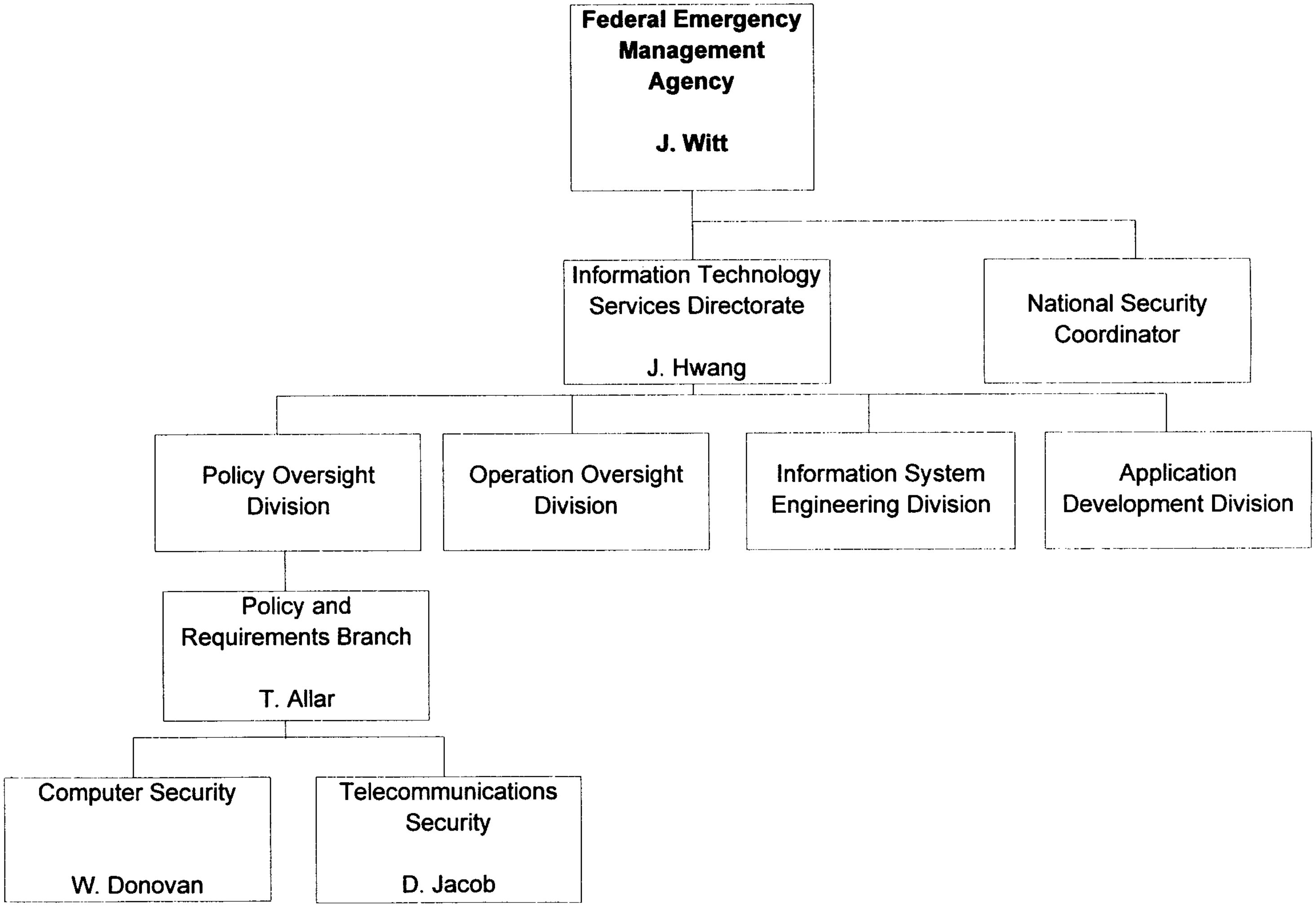
Emergency reporting requirements were levied by the FCC to learn immediately of significant service outages and to better determine whether particular technology, equipment or other changes may threaten service reliability. Outage reporting requirements have evolved since first established. Now, outages which potentially impact 30,000 customers for 30 minutes or more must be reported within 90 minutes. Additionally, outages which impact major airports, as defined by the FAA, major government and military facilities, nuclear power plants, and emergency 911 tandem switches must be reported. Outages involving nuclear power plants, government facilities and military facilities are reported through the National Coordinating Center. The initial report is made to the DISA Network Management Operations Center which contacts NCC staff members. NCC staff members evaluate the impact and report it to the FCC Watch Officer, if appropriate. Other outages are reported directly to the FCC Watch Officer in Washington DC. The FCC Field Office in Omaha, Nebraska provides backup to the Washington DC Watch office. Telephonic reports are followed by hard copy reports and final reports are due within 30 days.

FCC participates in the IITF. Mr. Neumann, and Mr. Kolly are involved in the Reliability and Vulnerability Working Group.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The FCC, as well as common carriers, are concerned with network reliability. They do not feel that they have responsibility for data security. The NRC has declined involvement in data security studies. This is viewed as a user responsibility.
- Outage reporting requirements have been developed in coordination with industry; particularly the NRC. Changes are implemented through the Federal Administrative Procedures Notice and Comment process.
- Carriers have initiated Mutual Aid Agreements in an effort to reduce the impact of service disruptions.

This page intentionally left blank.


Federal Emergency Management Agency
J. Witt
Information Technology Services Directorate
J. Hwang
National Security Coordinator
Policy Oversight Division
Operation Oversight Division
Information System Engineering Division
Application Development Division
Policy and Requirements Branch
T. Allar
Computer Security
W. Donovan
Telecommunications Security
D. Jacob

Organization: Federal Emergency Management Agency (FEMA)

Senior Information Assurance Official:

John Hwang, Associate Director, Information Technology Services Directorate (ITSD)

Information Assurance Points of Contact:

Tom Allar, Chief, Oversight Branch, Policy and Oversight Division, ITSD
Bill Donovan, Computer Security, Oversight Branch, Policy and Oversight Division, ITSD

Information Assurance Related Missions and Functions:

The Federal Emergency Management Agency (FEMA) is the central agency within the Federal Government for emergency planning, preparedness, mitigation, response, and recovery. FEMA funds emergency programs, offers technical guidance and training, and deploys Federal resources in time of catastrophic disaster. FEMA is also responsible for developing plans to ensure the continuity of the Federal Government during national security emergencies, and Federal response to the consequences of major terrorist incidents.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- A recent Agency reorganization created the Information Technology Services Directorate. This directorate retained many of the functions formerly performed by the Operations Support Directorate. The reorganization also consolidated most of the information systems development and operational activities from throughout the Agency in the Information Technology Services Directorate. The new Operations Support Directorate provides services in the areas of acquisition, administration, security, and logistics.
- An unclassified February 28, 1995, NSC memorandum states it is the policy of the Administration to continue the preparedness activities cited in Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 23, 1986. It further states that "Natural disasters and other emergencies, which may cause widespread or prolonged disruption of critical Federal Government functions, also warrant continued consideration as potential national security challenges" and that responsibilities "involve preparedness for any occurrence, including natural disaster, military attack, technological emergency or other emergency that seriously degrades or seriously threatens the national security." Finally, the memorandum charges FEMA with preparing "an assessment of the existing continuity of operations and continuity of government programs."
- FEMA information assurance activities are not fully developed because of budget and emphasis on response to natural and man-made disasters.
- Absolutely need an Executive Order to assign responsibilities in this area. Policy must include consequences for not following the policy. Health and Safety analog should be reviewed for possible application to the information area.

- Training and education regarding information assurance should be integrated into other training. In addition, this training should be mandatory. Senior leadership awareness, interest, and support is absolutely required! With size of government and the budget decreasing, we must emphasize awareness.
- Suggested forming a Federal Government organization which could provide advice and assistance regarding solutions to security problems. This organization should be centrally funded. NIST currently evaluates products but has restrictions on what information can be released to the government at large.
- Bare-bones internal information security policies are in place. Efforts are underway to improve existing policies.
- Donovan is the lone person responsible for developing and implementing computer security for FEMA.

This page intentionally left blank.

Federal Reserve System

Organization: Federal Reserve System (FRS)

Senior Information Assurance Official:

For Federal Reserve Banks:
Mr. Clyde H. Farnsworth, Jr.,'Director, Division of Reserve Bank Operations and Payment Systems

For Board of Governors:
Mr. Steven R. Malphrus, Division of Information Resources

Information Assurance Points of Contact:

Mr. John H. Parrish, Assistant Director, Division of Reserve Bank Operations and Payment Systems
Mr. Kenneth D. Buckley, Manager, Division of Reserve Bank Operations and Payment Systems
Mr. Raymond Romero, Project Leader, Division of Reserve Bank Operations and Payment Systems

Information Assurance Related Missions and Functions:

The Federal Reserve System is the central bank of the United States. it is charged by Congress with responsibility for conducting the nation's monetary policy; supervising and regulating banking institutions; maintaining the stability of the financial system; and providing certain financial services to the U.S. government, financial institutions, and foreign central banks. The Federal Reserve is also responsible for promoting efficiency in payment system practices.

In carrying out these responsibilities, the Federal Reserve executes monetary policy, examines commercial banks, transfers funds and government securities, handles government deposits and debt issues, acts as the lender of last resort, and a wide range of other activities. The System consists of seven parts: the Board of Governors, the twelve Federal Reserve Banks and their twenty-five branches, the Federal Open Market Committee, the Federal Advisory Council, the Consumer Advisory Council, the Thrift Advisory Council, and depository institutions.

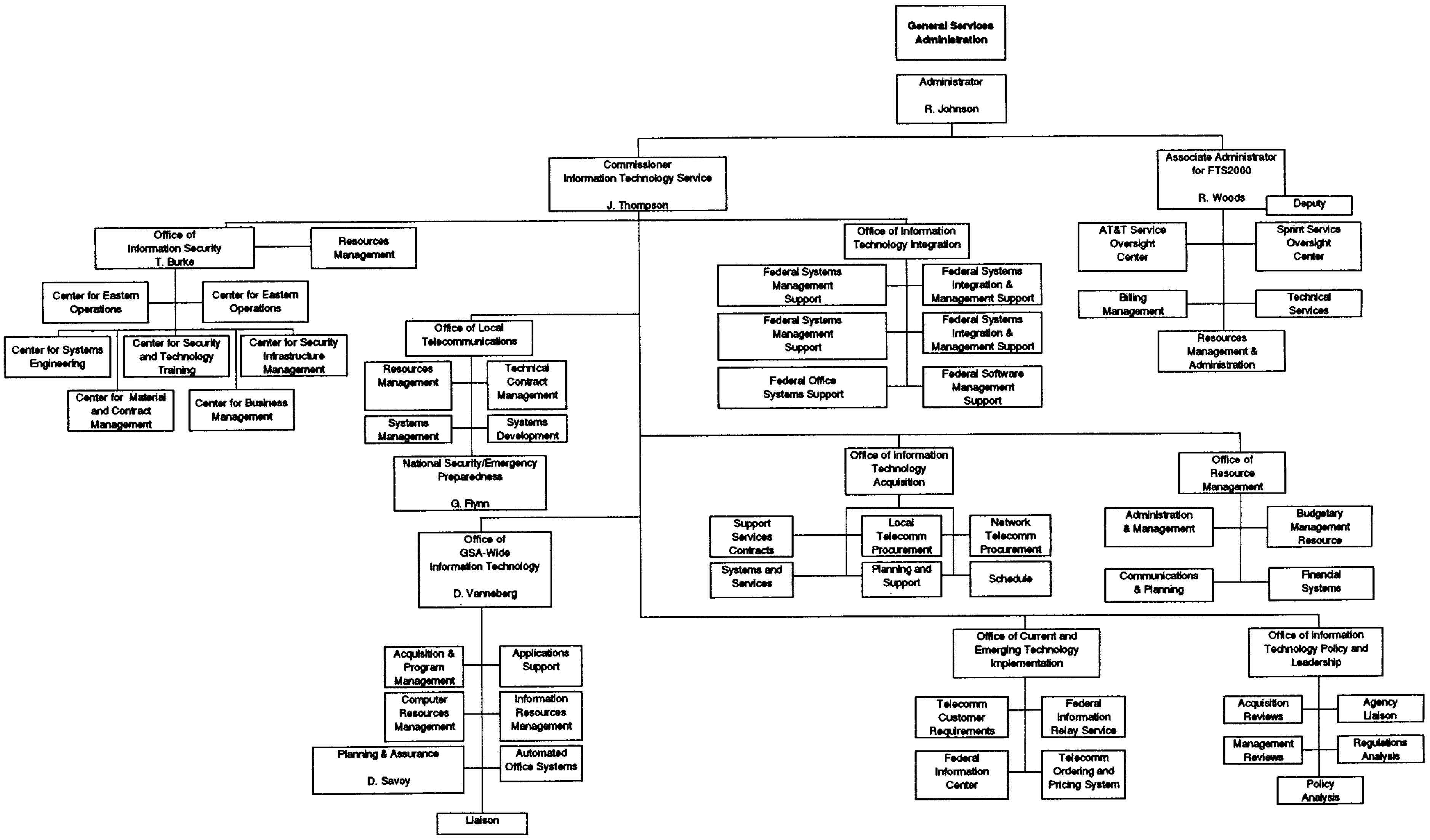
The Board of Governors exercises general supervision over Reserve Bank activities and examines each Reserve Bank annually. The Board approves minimum standards for data security in Reserve Banks, and the effectiveness of the Banks' implementation of controls is evaluated during the annual examinations and during internal audits.

The Board of Directors of each Federal Reserve Bank is composed of nine members: three represent the stockholding member banks and are elected by those banks; three represent commerce, agriculture, or industry in the district and are elected by the stockholding member banks; and three are appointed by the Board of Governors. The Board of Governors appoints one of these latter directors as Chairman of the Board of Directors and another as the Deputy Chairman.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- FRS was created as the Central Bank of the U.S. by act of Congress and is independent within government. Many checks and balances are used to oversee bank operations and maintain the integrity of the System. Parrish's office in the Division of Reserve Bank Operations and Payment Systems is responsible for advising the Board of Governors on the information security aspects of Reserve Bank operations.
- The Chief Operating Officers of each Federal Reserve Bank form a committee to deal with the many aspects of the FRS operation. The committee has in turn formed several working groups to deal with specialized and technical aspects of the FRS operation. One of these working groups is made up of the data security officers of each Federal Reserve Bank. This working group is responsible for developing and recommending security policy. The full committee approves the security policy which is implemented only with the concurrence of the Reserve Bank Operations and Payment Systems, acting on behalf of the Board of Governors.
- Each Federal Reserve Bank conducts internal audits, which include security reviews.
- The Board of Governors examines the Federal Reserve Banks on an annual basis. The Division of Reserve Bank Operations and Payment Systems has oversight responsibility with respect to the security operations of the Federal Reserve Banks.
- Recognition of the public responsibilities of the central bank drive a long-time organizational emphasis on integrity and effective controls in operations. Ownership of and accountability for information, need to know, separation of control, and custody of information procedures have been in place for decades to preserve that integrity. As manual procedures for processing physical valuables were automated over the years, appropriate controls were established for processing in the electronic environment.
- FRS operates three primary data centers and has extensive backup capabilities in the event of partial or whole site failures. Full disaster recovery plans are in place.
- FedWire is the real-time payments system application which provides over $200 trillion in funds transfer and government securities transactions between financial institutions a year. FedNet is the FRS network over which this traffic moves. Fedline is the link between financial institutions and FedWire.
- The Federal Reserve also oversees the Clearing House for Interbank Payments (CHIPS). This is a private sector multilateral net settlement clearing system operated by the New York Clearing House Association in New York City. It clears over $1 trillion a day.

This page intentionally left blank.


General Services Administration
Administrator
R. Johnson
Commissioner Information Technology Service
J. Thompson
Associate Administrator for FTS2000
R. Woods
Deputy
AT&T Service Oversight Center
Sprint Service Oversight Center
Billing Management
Technical Services
Resources Management & Administration
Office of Information Security
T. Burke
Resources Management
Center for Eastern Operations
Center for Eastern Operations
Center for Systems Engineering
Center for Security and Technology Training
Center for Security Infrastructure Management
Center for Material and Contract Management
Center for Business Management
Office of Local Telecommunications
Resources Management
Technical Contract Management
Systems Management
Systems Development
National Security/Emergency Preparedness
G. Flynn
Office of GSA-Wide Information Technology
D. Vanneberg
Acquisition & Program Management
Applications Support
Computer Resources Management
Information Resources Management
Planning & Assurance
D. Savoy
Automated Office Systems
Liaison
Office of Information Technology Integration
Federal Systems Management Support
Federal Systems Integration & Management Support
Federal Systems Management Support
Federal Systems Integration & Management Support
Federal Office Systems Support
Federal Software Management Support
Office of Information Technology Acquisition
Support Services Contracts
Local Telecomm Procurement
Network Telecomm Procurement
Systems and Services
Planning and Support
Schedule
Office of Resource Management
Administration & Management
Budgetary Management Resource
Communications & Planning
Financial Systems
Office of Current and Emerging Technology Implementation
Telecomm Customer Requirements
Federal Information Relay Service
Federal Information Center
Telecomm Ordering and Pricing System
Office of Information Technology Policy and Leadership
Acquisition Reviews
Agency Liaison
Management Reviews
Regulations Analysis
Policy Analysis

Organization: General Services Administration (GSA)

Senior Information Assurance Official:

Mr. Joe M. Thompson, Commissioner, Information Technology Service, GSA

Information Assurance Points of Contact:

Mr. Thomas Burke, Deputy Commissioner, Office of Information Security, GSA
Mr. G. Flynn, National Security Emergency Preparedness, Office of Local Telecommunications, GSA
Mr. R. Woods, Associate Administrator for FTS2000, GSA
Mr. D. Venneberg, Deputy Commissioner, Office of GSA-Wide Information Technology, GSA
Ms. Diane Savoy, Planning and Assurance Division, Office of GSA-Wide Information Technology, GSA
Mr. Bruce Brignall, Post FTS2000 Acquisition Strategy, Office of the Associate Administrator for FTS2000

Information Assurance Related Missions and Functions:

The General Services Administration establishes policy for and provides economical and efficient management of Government property and records, including construction and operation of buildings, procurement and distribution of supplies, utilization and disposal of property; transportation, traffic, and communications management; and management of the Governmentwide automatic data processing resources program. It consists of operating services and support staff offices, with functions carried out at three levels of organization: the central office, regional offices, and field activities.

The Office of Acquisition Policy has a major role in developing, maintaining, issuing, and administering guiding principles via the Federal Acquisition Regulation (FAR) which is applicable to all Federal agencies.

The Office of the Associate Administrator for FTS2000 provides common-user telecommunications and other information services to agencies of the Federal Government.

The Information Security Oversight Office is responsible for overseeing executive branch agencies' actions to implement Executive Order 12356, April 2, 1982, which prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

The Office of Information Technology Services provides a variety of services related to information assurance. The office is responsible for coordination and direction of a comprehensive, Government-wide program for the management, procurement, and utilization of automated data processing and local telecommunications equipment and services. The Office of Information Technology Integration provides technical and contracting assistance through three complementary programs: the Federal Systems Integration and Management System (FEDSIM); the Federal Computer Acquisition Center (FEDCAC); and the Federal Information System Support Program (FISSP). The Agency Management Assistance Office conducts several management assistance programs that assist agencies in improving their information-related functions and activities. Among these is the Trail Boss program that helps Federal agencies prepare for major acquisitions. The Information Resources Management Policy Office is responsible for coordinating policy making activities related to information functions and authorities. This office develops, coordinates, and issues Governmentwide automatic data processing and telecommunications acquisition management and use regulations, the Federal Information Resources Management Regulations (FIRMRs). The Information Resources Procurement Office plays a major role in the Governmentwide procurement of automatic data processing and telecommunications hardware, software, and services. In some instances, this office issues a Delegation of Procurement Authority (DPA) which permits Federal agencies to procure their own hardware, software, and services. The Office of Telecommunications Services plays a major role in Governmentwide activities to improve the interagency Information Resources Management (IRM) infrastructure through the Interagency IRM Infrastructure Task Group. This office also manages and administers the National Security Emergency Preparedness Telecommunications Program activities.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Office of Information Security (OIS) was organized in October 1994, but the services this office provides have been provided by GSA since 1962 beginning with support to the Atomic Energy Commission.
- OIS provides a full spectrum of security services on a reimbursable basis to any customer in the Federal Government. The services include engineering, installation, operation and maintenance, systems administration, network management, and a secure packet switching network as a part of FTS 2000. OIS is capable of quick reaction support. The office receives no appropriated moneys. DoD constitutes approximately 60-70 percent of the OIS business and the numbers are growing. Other customers include FBI Legal Attaches, FAA, and the Defense Logistics Agency. These security services support C2, law enforcement operations, regulatory, political, and economic activities, and intelligence operations. OIS also provided coalition warfare support during Desert Shield/Storm and currently supports NATO and UN missions in the Balkans.
- OIS has a long-standing relationship with the National Security Agency (NSA) and the National Institute for Standards and Technology. OIS is currently providing support to the Multilevel Information Systems Security Initiative (MISSI) prototype and to the public key infrastructure prototype. This support includes life-cycle support planning.
- OIS represents GSA in the Information Infrastructure Task Force's (IITF) Security Issues Forum (SIF). OIS participates as a full member in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and an OIS representative co-chairs, with Treasury, the National Information Infrastructure (NII) Task Force of the NSTISSC. OIS also participates in the Federal Agency Computer

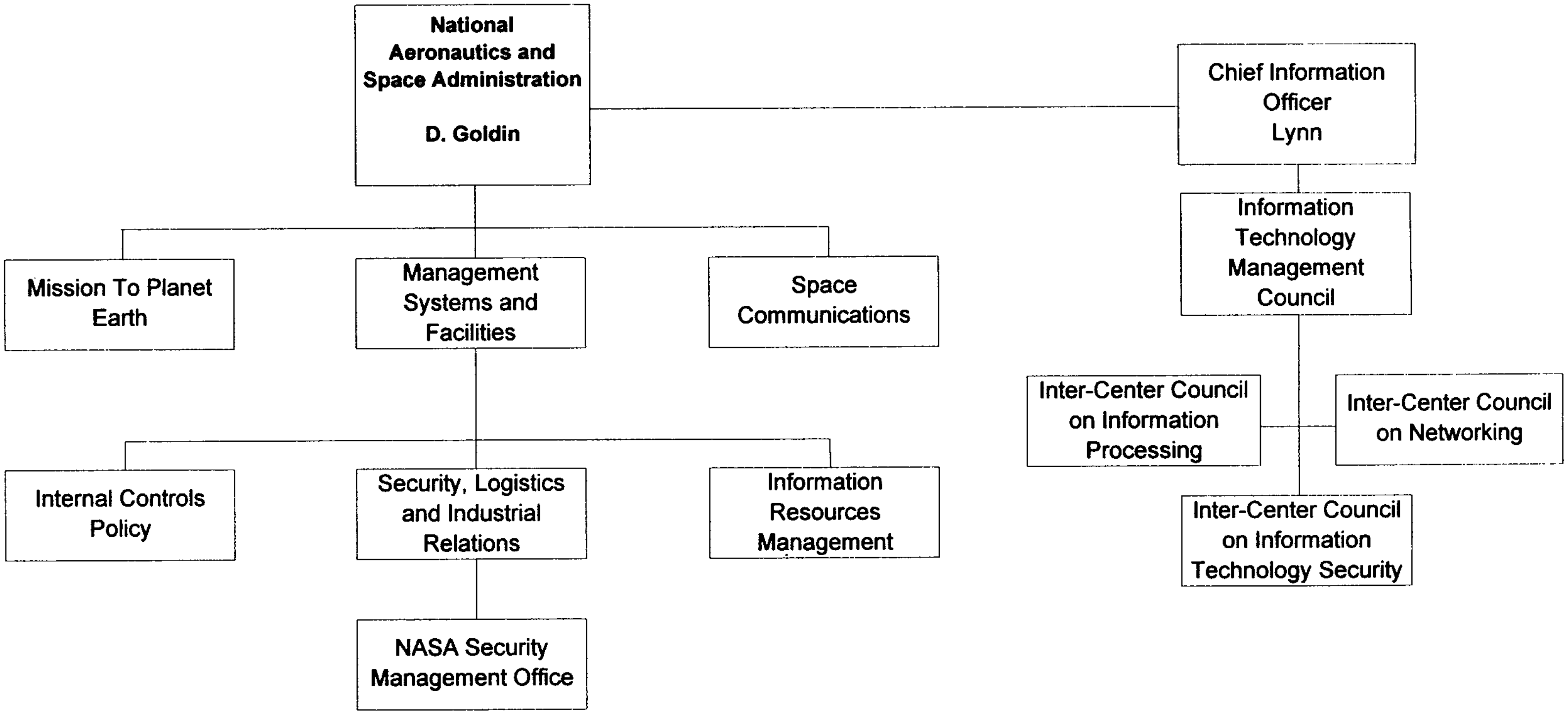
Security Program Manager's Forum (FACSPMF). OIS also represents GSA on the Military Communications Electronic Board.

- GSA has three resident program management offices which are chartered by interagency coordinating activities and empowered by agencies and activities having related responsibilities. The offices are the Electronic Commerce Program Management Office (co-chaired by DoD and GSA), the Electronic Mail Program Management Office (chaired by GSA), and the Security Infrastructure Program Management Office which was formed when numerous electronic commerce and electronic mail security issues (such as access control, integrity, non-repudiation, and confidentiality) surfaced. The Electronic Commerce PMO and the Electronic Mail PMO were chartered by the Government Information Technology Services Working Group which supports the Committee on Applications and Technology of the Information Infrastructure Task Force. In addition, the ECPMO was chartered by the Office of Federal Procurement Policy of the Office of Management and Budget. The Security Infrastructure PMO is co-chaired by GSA and DoD. Intended staffing is approximately 20 people with the staffing being shared among GSA, DISA, NSA, DoJ, Treas, and USPS.
- OIS conducts technical training.
- Issues: Guard technology to allow OIS LAN to interconnect with networks outside the controlled OIS office space.
- Lessons Learned: McAffe network virus checker is identifying viruses other virus checkers should have identified, but did not.
- Information security policy development for GSA is done by the Assurance Division of the Office of GSA-Wide Information Technology. Policy directives in the form of manuals, handbooks, etc. have been published and cover the traditional areas of computer security.
- Brignull operates an interagency group responsible for developing Post FTS2000 acquisition strategy.
- This group is attempting to reach out to the user community to determine needs for Post FTS2000. They have conducted a requirements call and several round tables to address issues such as security and interoperability, wireless services, 800/900 services, data, international, and billing.
- The group seems convinced that there are infrastructure vulnerability problems, but is not sure how to solve them. Possible avenues are legislation, regulation, market forces, and promulgation of industry best practices. Community will also need the help of NIST and NSA.
- The Reliability and Vulnerability Working Group, Telecommunications Policy Committee, Information Infrastructure Task Force, is working on some of the issues. Working group includes has panels working on risk management (chaired by Phil Quaid of NSA), reliability (chaired by Don Nichols of GSA), and standards (chaired by NIST).
- Some of the security and interoperability roundtable issues included warning screens for protected environments, priorities for restoration of services, privacy of billing information, and practicality of standards such as the digital signature standard.
- Of note, cable TV vendors have been added to the FCC's Network Reliability Council and an international subcommittee has also been added to try to collect international

outage information. A recommendation has also been made that a security subcommittee be added.

- The Planning and Assurance Division, Office of GSA-Wide Information Technology, is responsible for writing IT systems security policy for GSA internal operations. The Division recently issued policy guidance on use of Internet. It has also recently distributed through electronic mail a policy directive forbidding the downloading of SATAN. Policy directives are issued in the form of GSA Orders, Memos, and IT Program Updates.

This page intentionally left blank.


National Aeronautics and Space Administration
D. Goldin
Chief Information Officer
Lynn
Mission To Planet Earth
Management Systems and Facilities
Space Communications
Information Technology Management Council
Inter-Center Council on Information Processing
Inter-Center Council on Networking
Inter-Center Council on Information Technology Security
Internal Controls Policy
Security, Logistics and Industrial Relations
Information Resources Management
NASA Security Management Office

Organization: National Aeronautics and Space Administration

Senior Information Assurance Official:

Daniel S. Goldin, Administrator
John Lynn, Chief Information Officer
Benita A. Cooper, Associate Administrator for Management Systems and Facilities

Information Assurance Points of Contact:

Jeffrey E. Sutton, Director, Security, Logistics, and Industrial Relations Division
Russell S. Rice, Director, Information Resources Management Division
Mark J. Barai, Director, NASA Security Management Office
Richard W. Carr, NASA Information Technology Security Program Manager

Information Assurance Related Missions and Functions:

The National Aeronautics and Space Administration conducts research for the solution of problems of flight within and outside the Earth's atmosphere and develops, constructs, tests and operates aeronautical and space vehicles. It conducts activities required for the exploration of space with manned and unmanned vehicles and arranges for the most effective utilization of the scientific and engineering resources of the United States with other nations engaged in aeronautical and space activities for peaceful purposes.

The Office of Mission to Planet Earth conducts NASA's programs that study global climate change and integrated functioning of the Earth as a system. This includes developing and managing remote sensing satellites and instruments, aircraft and ground measurements and research, as well as data and information systems needed to support the objectives of the U.S. Global Change Research Program.

The Office of Space Communications is responsible for meeting requirements critical to NASA's aeronautics and space flight missions. They include spacecraft operations and control centers, ground and space communications, data acquisition and processing, flight dynamics and trajectory analyses, spacecraft tracking and applied research, and development of new technology. A global communications system links tracking sites, control centers, and data processing facilities that provide real-time data processing form mission control, orbit and attitude determination, and routine processing of telemetry data for space missions.

The Goddard Space Flight Center develops and operates information systems technology. The Jet Propulsion Center conducts mission operations and ground based research in information systems technology. The Langley Research Center performs technology experiments in remote sensor and data acquisition and communication technology. The Lewis Research Center conducts research in controls and electronics.

The Associate Administrator for Management Systems and Facilities has overall responsibility for information security and information resource management operations The NASA Security Management Office is a part of the Security, Logistics and Industrial Relations Division. The Security Management Office is responsible for policy development and management oversight for communications, automated information, personnel, physical, information, industrial, and operations security. Responsibility for Information Technology Security technical integration, implementation, and operation resides in the NASA Information Resources Management Office.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NASA has an extensive Information Technology Security program that is integrated into its management functions through management points-of-contact, intraagency working groups, councils, and committees. The goal of the program is to provide cost-effective protection that assures high integrity ready availability, and confidentiality of NASA automated information resources. The program consists of the following basic elements:
    - Policy and guidance
    - Planning
    - Sensitivity and criticality identification
    - Risk management
    - Protection measures baseline
    - Certifications and re-certifications
    - Compliance assurance
    - Incident response
    - Awareness and training
- Due to NASA's decentralized approach to managing its diverse, global computer and network environments, it has adopted a decentralized approach to implementing its ITS program. NASA headquarters interprets national policy and guidance and issues general policy and guidance internally. Each program office is responsible for establishing an information technology security management function which ensures the security, integrity, and continuity of operations for automated information resources directly related to program missions. Each Center and Data Processing Installation is responsible for establishing and sustaining an information technology security program that assures each data processing center under its management complies with security requirements that are consistent with its mission.
- Each Center is responsible for establishing a Computer (and Network) Security Incident Response (CSIR) capability, which is integrated with the Center's Technical Help Desk facility to provide coverage for local computer systems and local area networks. In addition, NASA has an Agency-wide incident response capability (the NASA Security Incident Response Capability (NASIRC)) which has been in existence at the Goddard Space Flight Center for the past two years.
- NASA has instituted a rigorous risk assessment process that includes determining the relative value, sensitivity, and criticality of information, computing, and communications resources. Various protection, detection, and reaction measures are applied to

information, communications, and computing resources based on the criticality of various categories of information (e.g., information about persons, mission-critical information) based on the impact loss or destruction of the information or resources might have.

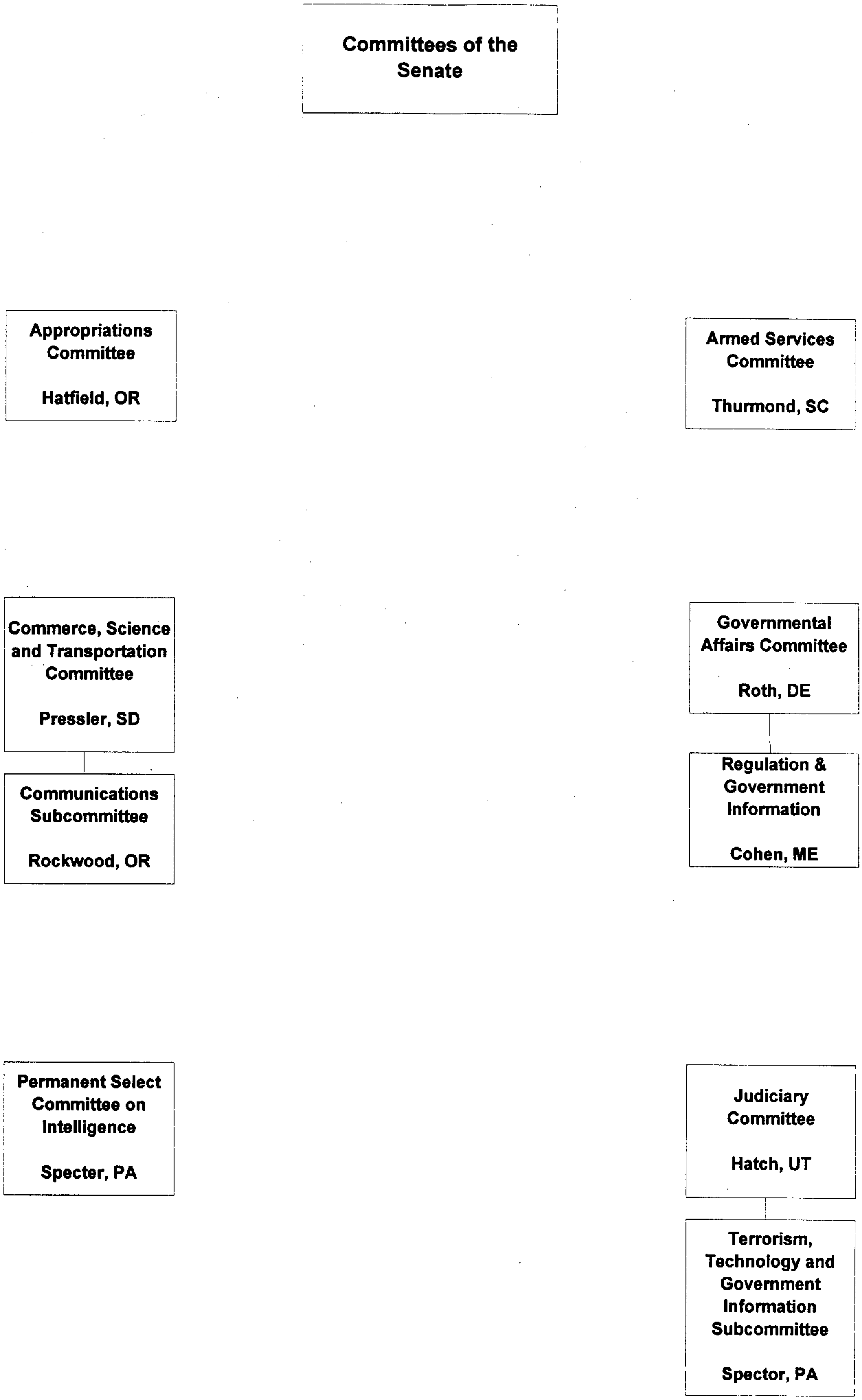
- NASA participates in a variety of interagency information technology security activities to include National Security Telecommunications and Information Systems Security Committee (NSTISSC), the Information Infrastructure Task Force Security Issues Forum (SIF), Information Systems Security Organization (ISSO), National Institute of Standards and Technology (NIST) Working Groups, and the Forum of Incident Response and Security Teams (FIRST)
- An effective Agency information technology security program must have top-down senior management support and be appropriately placed in the organizational management structure so that it gets the visibility, attention, and resources it needs to get the job done -- and eliminate unnecessary political conflicts of interest.
- An issue of significant importance to NASA is the capability to conduct business electronically. In order to conduct official business (to include typical commerce activities) over the National Information Infrastructure and the Internet, capabilities must exist for effectively and efficiently applying a digital signature to documents and enclosing those documents in a security envelope to prevent unauthorized disclosure or manipulation of the document.

This page intentionally left blank.

Independent Establishments and Government Corporation
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Central Intelligence Agency			Gerschwin	Larry			703-482-7424	
Central Intelligence Agency			Wantanabe	Frank			703-874-0392	
Central Intelligence Agency			Welch	Jasper			703-556-7233	
Central Intelligence Agency			Zimmerman	Mark			703-874-0392	
Federal Communications Commisssion (FCC)			Hundt	Reed		Chairman		
Federal Communications Commisssion (FCC)			Kolly	Roy			202-418-1150	
Federal Communications Commisssion (FCC)			Neumann	Herb			202-634-1373	
Federal Communications Commisssion (FCC)			Van Doorn	Arlan			202-632-7200	
Federal Emergency Management Agency (FEMA)	Policy Oversight Branch		Allar	Tom			202-646-2984	
Federal Reserve System (FRS)	Board of Governors of the Federal Reserve Board		Parrish	John		Assistant Director, Information	202-452-2224	NCS COP
Federal Reserve System (FRS)			Buckley	Ken			202-452-3646	
Federal Reserve System (FRS)			Romero	Ray			202-452-2832	
General Services Administration (GSA)	Office of Information Security		Burke	Tom		Deputy Commissioner	202-708-7000	
General Services Administration (GSA)			Flynn	George			202-501-0843	
National Aeronautics and Space Administration (NASA)			Carr	Rick		Information Technology Security Program Manager	202-358-2309	

This page intentionally left blank.



Committees of the Senate

Appropriations Committee

Hatfield, OR

Armed Services Committee

Thurmond, SC

Commerce, Science and Transportation Committee

Pressler, SD

Communications Subcommittee

Rockwood, OR

Governmental Affairs Committee

Roth, DE

Regulation & Government Information

Cohen, ME

Permanent Select Committee on Intelligence

Specter, PA

Judiciary Committee

Hatch, UT

Terrorism, Technology and Government Information Subcommittee

Spector, PA

Organization: Senate

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may effect activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

Committee/Subcommittee: Appropriations Committee

Chairman: Sen. Hatfield, Oregon

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- The Committee is faced with funding the Communications Assistance for Law Enforcement Act of 1994. The act mandated but did not appropriate $500 Million over five years to refund to carriers the cost of modifying their equipment.
- Expected to cut DoC operating budget for telecommunications projects such as the NTIA, NII grants, and Advanced Technology Project.

Committee/Subcommittee: Armed Services Committee

Chairman: Sen. Thurmond, South Carolina

Information Assurance Related Missions and Functions:

Defense budget authorization.

Information Assurance Activities:

Committee/Subcommittee: Committee on Commerce, Science and Transportation

Chairman: Sen. Pressler, South Dakota

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Approved a draft of the Telecommunications Competition and Deregulation Act of 1995 on March 30, 1995.

Committee/Subcommittee: Commerce Subcommittee on Communications

Chairman: Sen. Packwood, Oregon

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Committee

Chairman: Sen. Roth, Delaware

Information Assurance Related Missions and Functions:

Privacy Act, regulatory issues, government performance and results

Information Assurance Activities:

- Introduced acquisition reform legislation in coordination with the House Budget Committee.
- Introduced regulatory reform legislation. Proposed legislation will require FCC, and other regulatory agencies, to conduct "regulatory impact analysis" of any regulation that will impact the economy over $100 Million annually or significantly increase prices or adversely impact competition.
- Sen. Roth sponsored the Government Performance and Results Act. He sees performance measurement as the key to improving federal government management.

Committee/Subcommittee: Governmental Affairs Subcommittee on Regulation and Government Information

Chairman: Sen. Cohen, Maine

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Pending legislation to overhaul the Federal Government's IT management structure.
  Requires agency chief information officers and a new IT oversight office in OMB.
- Sen. Cohen sees information technology as the key to improving federal government management.

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Sen. Hatch, Utah

Information Assurance Related Missions and Functions:

Information Assurance Activities:

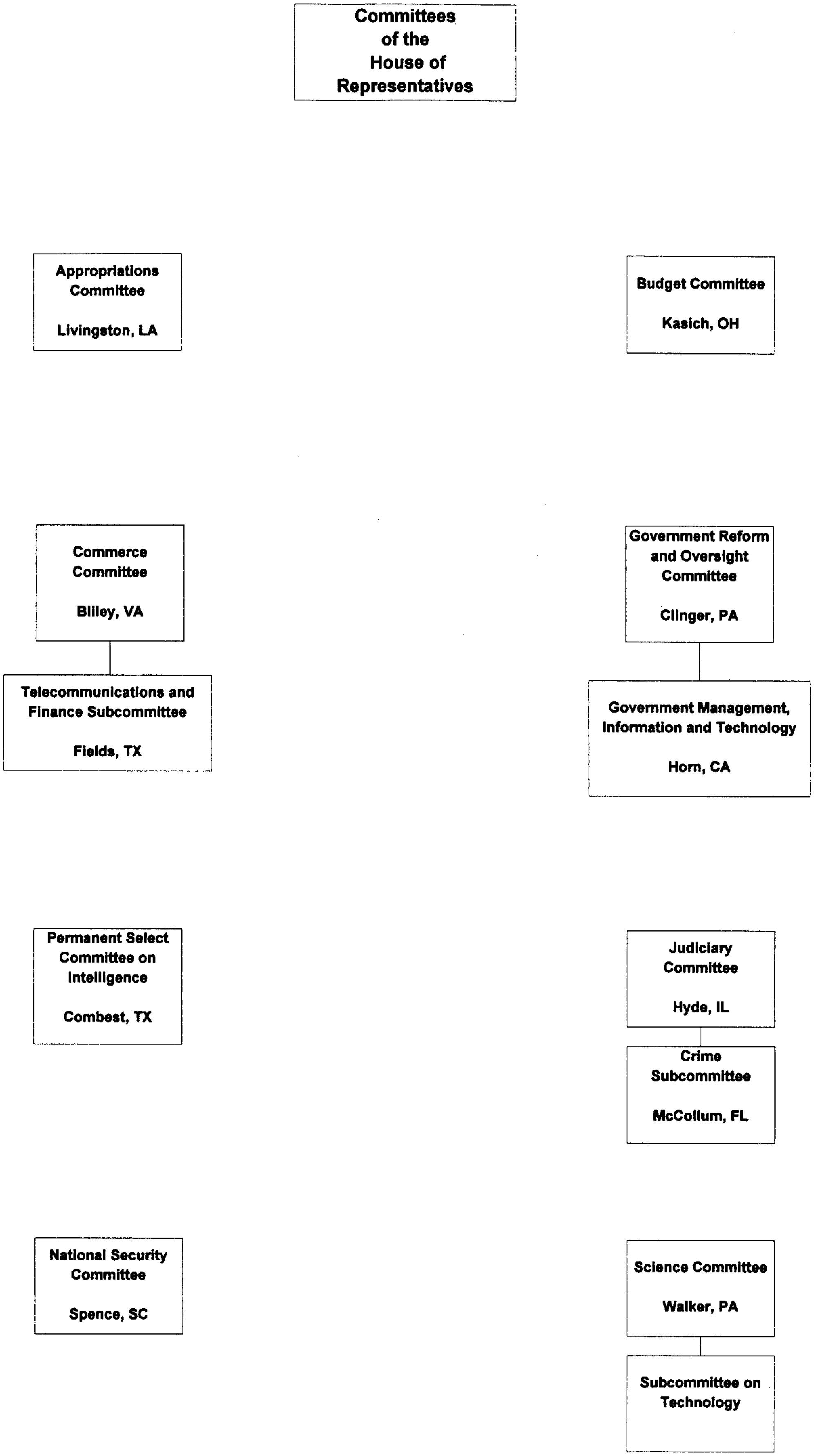
Committee/Subcommittee: Judiciary Subcommittee on Terrorism, Technology and Government Information

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Pending legislation on how the government buys hardware and software.



Committees of the House of Representatives

Appropriations Committee

Livingston, LA

Budget Committee

Kasich, OH

Commerce Committee

Bliley, VA

Telecommunications and Finance Subcommittee

Fields, TX

Government Reform and Oversight Committee

Clinger, PA

Government Management, Information and Technology

Horn, CA

Permanent Select Committee on Intelligence

Combest, TX

Judiciary Committee

Hyde, IL

Crime Subcommittee

McCollum, FL

National Security Committee

Spence, SC

Science Committee

Walker, PA

Subcommittee on Technology

Organization: House of Representatives

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may affect IW activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

Committee/Subcommittee: Appropriations Committee

Chairman: Rep. Livingston, Louisiana

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

Committee/Subcommittee: Budget Committee

Chairman: Rep. Kasich, Ohio

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

- Introduced acquisition reform legislation in coordination with the Senate Governmental Affairs Committee.

Committee/Subcommittee: Commerce Committee

Chairman: Rep. Bliley, Virginia

Information Assurance Related Missions and Functions:

Federal Communications Commission

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Telecommunications and Finance

Chairman: Rep. Fields, Texas

Information Assurance Related Missions and Functions:

Privacy, telecommunications, finance

Information Assurance Activities:

- Expected to offer legislation on Caller ID, telemarketing, cable TV, and a "Privacy Bill of Rights"
- Prepared House Telecommunications Reform Bill

Committee/Subcommittee: Government Reform and Oversight Committee (formerly Government Operations Committee)

Chairman: Rep. Clinger, Pennsylvania

Information Assurance Related Missions and Functions:

Civil Service, Postal Service, Washington DC, oversight

Information Assurance Activities:

- Rep. Clinger plans to take the lead role in communicating federal agency information technology needs to the House.
- Rep. Clinger cosponsored the Paperwork Reduction Act.

Committee/Subcommittee: Government Reform and Oversight Subcommittee on Government Management, Information, and Technology (New subcommittee)

Chairman: Rep. Horn, California

Information Assurance Related Missions and Functions:

Privacy Act, NII, paperwork reduction, Federal Agencies

Information Assurance Activities:

- Possible hearings on Post-FTS2000.
- Planned hearings on Acquisition Streamlining Act of 1994 and purchase of IT equipment and services.

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Rep. Combest, Texas

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Rep. Hyde, Illinois

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Judiciary Subcommittee on Crime

Chairman: Rep. McCollum, Florida

Information Assurance Related Missions and Functions:

FBI, criminal justice

Information Assurance Activities:

Committee/Subcommittee: Committee on National Security (Formerly House Armed Services Committee)

Chairman: Rep. Spence, South Carolina

Information Assurance Related Missions and Functions:

Defense Budget "authorizers"

Information Assurance Activities:

Committee/Subcommittee: Science Committee

Chairman: Rep. Walker, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Rep. Walker is concerned that U.S. standards process is limiting international trade.
- May propose legislation to establish a Department of Science to consolidate technology programs at DoE and DoC, as well as NASA, EPA, and National Oceanic and Atmospheric Administration.
- Expected to cut National Science Foundation budget by as much as 50%.

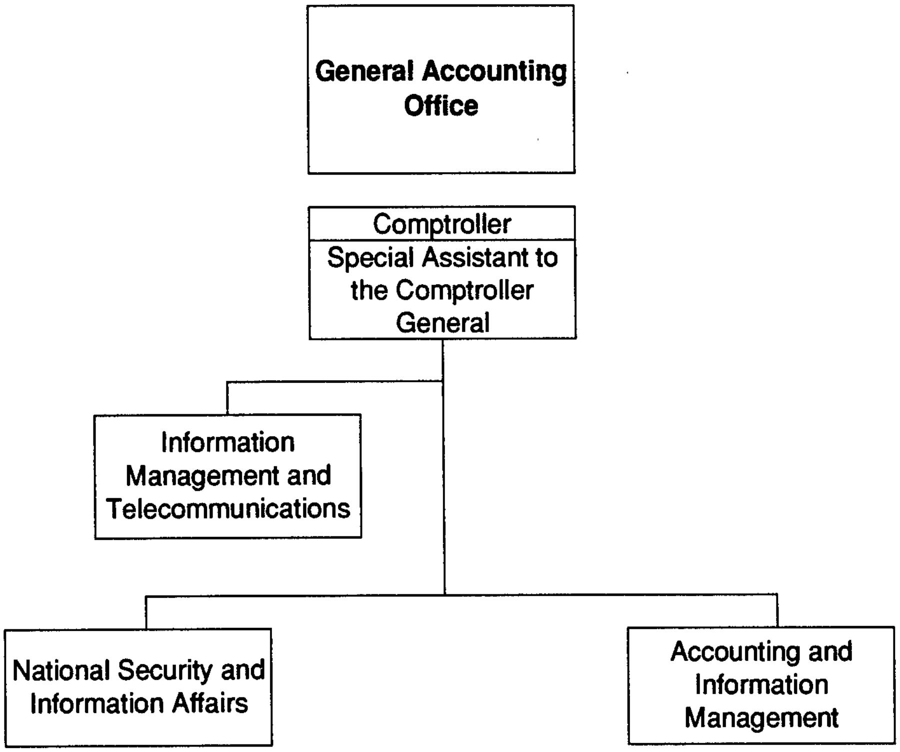
Committee/Subcommittee: Science Subcommittee on Technology

Chairman: Rep Morella, Maryland

Information Assurance Related Missions and Functions:

Information Assurance Activities:

This page intentionally left blank.


General Accounting Office
Comptroller
Special Assistant to the Comptroller General
Information Management and Telecommunications
National Security and Information Affairs
Accounting and Information Management

Organization: General Accounting Office

Senior Information Assurance Officials:

F. Kevin Boland, Assistant Comptroller General, Office of Information Management and Communications
Jack Brock, Director of Information Resources Management
Frank C. Conohan, Assistant Comptroller General, National Security and International Affairs Division

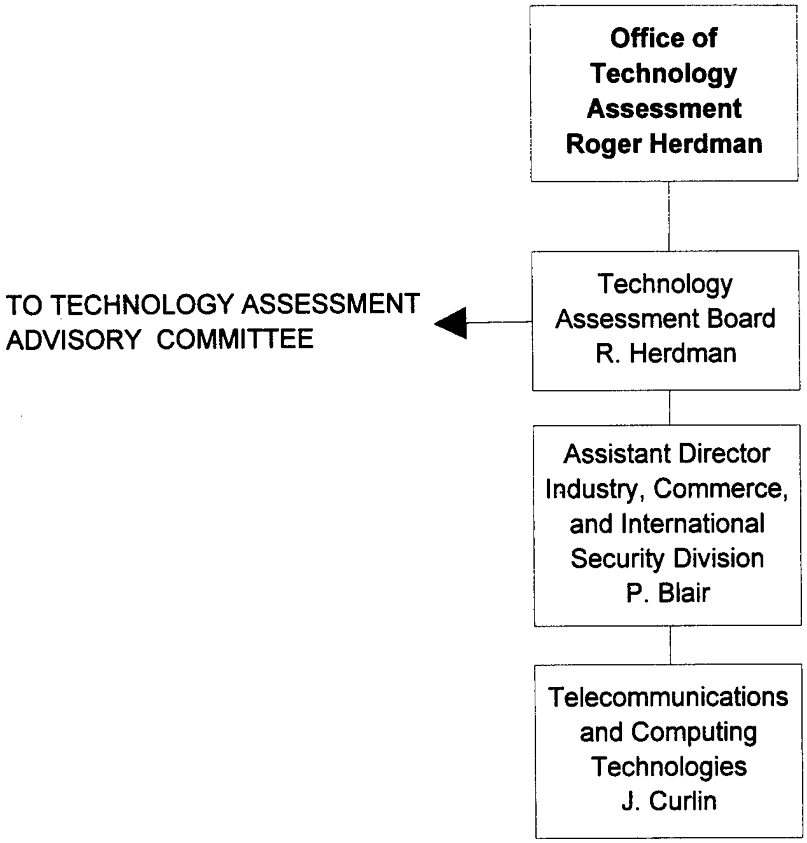
Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The General Accounting Office (GAO) is the audit and investigative arm of the Congress. Its primary function is to respond to requests from Congress for audits and evaluations of government programs and agencies. The GAO also works closely with the Office of Management and Budget and the Secretary of the Treasury to standardize federal government information systems. The GAO also prescribes accounting standards for the Executive Branch.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- GAO continues to find examples of poor information security during audits and investigations.
- Reports issued in 1989, 1991, and 1993 highlight problems with virus' on the Internet, privacy invasions by federal employees, and penetrations of DoD computer systems (Appendix B, Other References).
- Internally, GAO has installed Internet connections with firewalls.


Office of Technology Assessment Roger Herdman
Technology Assessment Board R. Herdman
TO TECHNOLOGY ASSESSMENT ADVISORY COMMITTEE
Assistant Director Industry, Commerce, and International Security Division P. Blair
Telecommunications and Computing Technologies J. Curlin

Organization: Office of Technology Assessment

Senior Information Assurance Official:

James Curlin, Program Director, Telecommunications and Computing Technologies

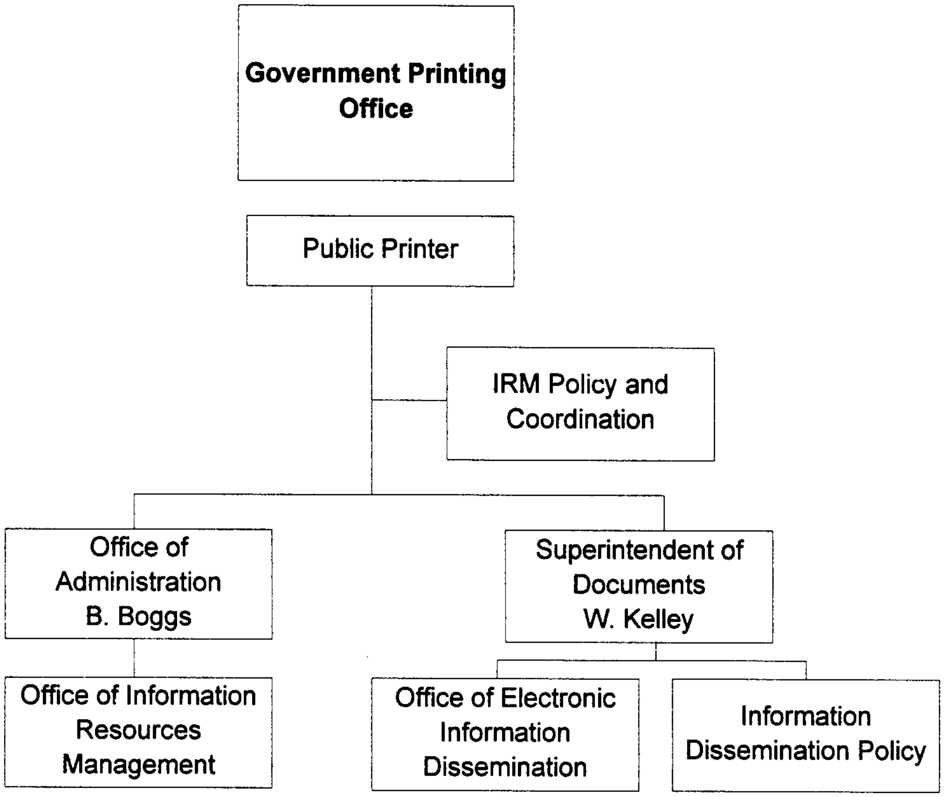
Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The Office of Technology Assessment (OTA) "reports to Congress on the scientific and technical impact of government policies and proposed legislative initiatives." [Office of the Federal Register, 1994] It receives guidance and assignments from a Congressional Board and advice from a Technology Assessment Advisory Council. Its assessments are comprehensive; often taking one to two years to complete, and authoritative as each OTA assessment team is advised by a panel of experts.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OTA reports are comprehensive, authoritative, and readable and are available from the U.S. Government Printing Office. (Appendix B, Other References)


Government Printing Office
Public Printer
IRM Policy and Coordination
Office of Administration B. Boggs
Superintendent of Documents W. Kelley
Office of Information Resources Management
Office of Electronic Information Dissemination
Information Dissemination Policy

Organization: Government Printing Office

Senior Information Assurance Officials:

Vacant, Office of Information Resources Management, Office of Administration
Judith Russell (Acting), Office of Electronic Dissemination, Superintendent of Documents

Information Assurance Points of Contact:

Information Assurance Related Missions and Functions:

The Government Printing Office (GPO) prints, binds, and distributes documents for the Federal government. It has special statutory authority to make documents available electronically to the public free of charge. It is better known for selling government publications through mail order and GPO bookstores at reasonable prices. It also produces and provides documents on CD-ROM, operates File Transfer Protocol and World Wide Web sites and makes information available through the Federal Bulletin Board.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.

Legislative and Judicial
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
House of Representatives	House Appropriations Committee	Survey and Investigative Staff	Baker	T	Keith		351-2567	
House of Representatives	House Appropriations Committee	Survey and Investigative Staff	Haures	Carroll				
House of Representatives	House Appropriations Committee		Lilly	R	Scott	Staff Director	202-225-3481	
House of Representatives	House Appropriations Committee	Survey and Investigative Staff	Mullenhoff	Paul				
House of Representatives	House Government Reform and Oversight	Government Management, Information and Oversight Subcommittee	George	T	Russell	Staff Director	202-225-5147	General information technology issues.
House of Representatives	House Oversight Committee		Pockros	Perry			202-225-2061	
House of Representatives	House Science Committee		Paul	James			202-226-3639	General information technology issues.
Office of Technology Assessment			Wye	David		Project Director for Wireless Technology and the National Information Infrastructure	202-224-3695	Internet issues.
Senate	Commerce, Science & Transportation Committee		Windham	Pat			202-224-0411	General information technology issues.
Senate	Senate Appropriations Committee		Cohen	Debbie		Legislative Assistant		R-Ore; Chairman, Appropriations Committee
Senate	Senate Appropriations Committee		Hatfield	Mark		Senator		
Senate	Senate Appropriations Committee		Morrison	David			202-224-7296	Procurement and Info Technogy issues for Sen Glenn, ranking Democrat on Senate Gov't Affairs Committee.
Senate	Senate Governmental Affairs Committee		Foreman	Mark			202-224-4751	Information Management programs for the Defense Subcommittee.

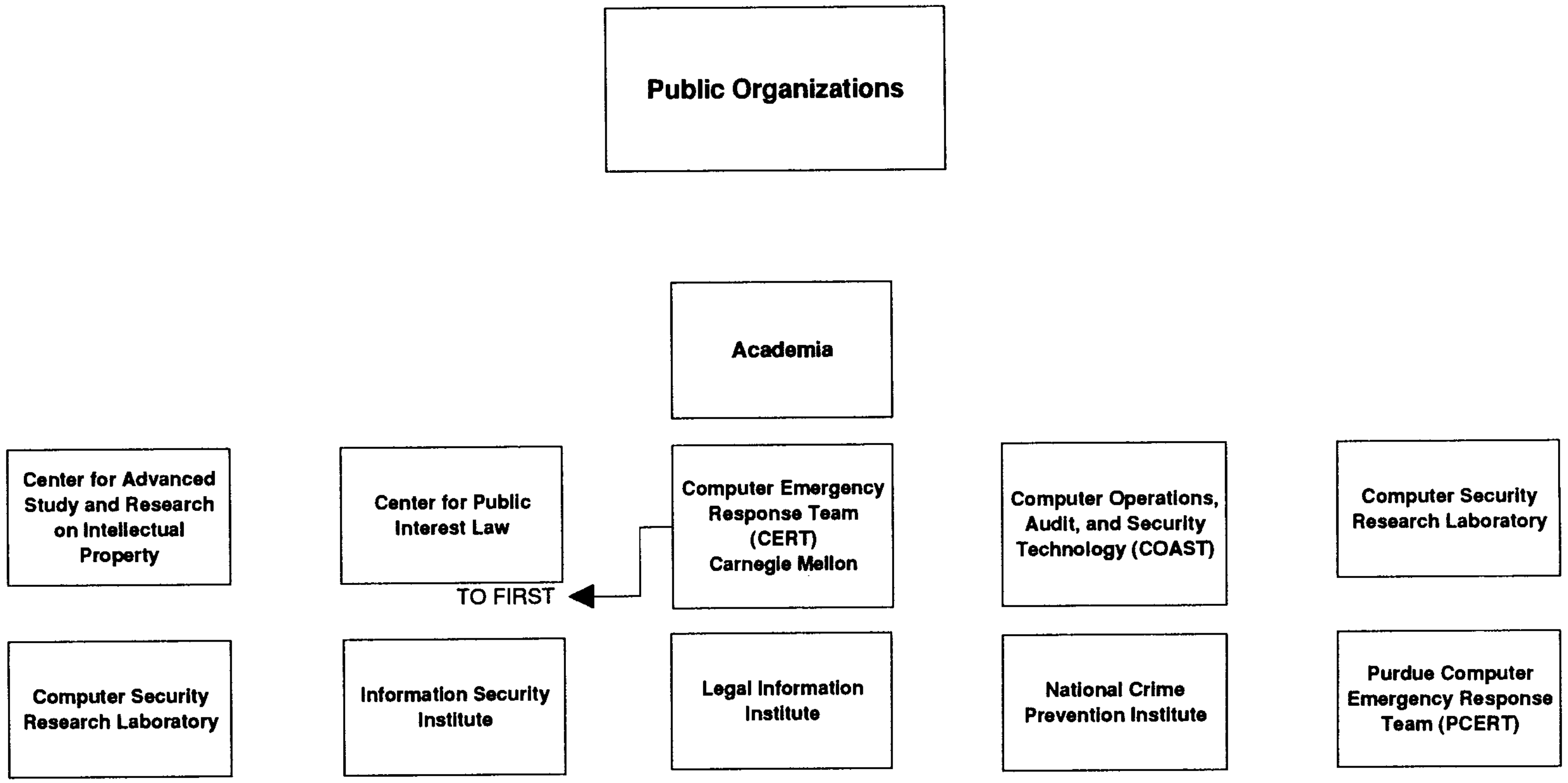
This page intentionally left blank.

International
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Canadian Department of National Defence	DITIS 4 ADM(DIS)/DGISO		Boot	D	N	I.T.I. Security Manager	613-990-5284	2nd Int'l Conf on IW, Jan 95 participant
Canadian Government	Office of the Privacy Commission of Canada		Foran	Brian		Special Advisor	800-267-0441	2nd Int'l Conf on IW, Jan 95 participant
Canadian Security Intelligence Service	Analysis and Production Branch		Porteous	Samuel		Strategic Analyst	613-782-1002	2nd Int'l Conf on IW, Jan 95 participant
Department of National Defence	Information Security	Communications Security Establishment	Pickering	Alan		Director General of Information Security	613-991-7176	CSE is Canada's equivalent to NSA; Attended the NCSA Conf, Jan 95 participant
Department of National Defence, Canada	Defence Information Services Organization		Garigue	Robert	J	Strategic Information Advisor to ADM	613-992-6855	2nd Int'l Conf on IW, Jan 95 participant
Federal Republic of Germany	Ministry of Posts and Telecommunications		Botsch	Wolfgang		Federal Minister		Germany will allow wholesale competition in telecommunications in 1998.
LGS Group Inc.			Kabay	Michel	E	Management Consultant	514-861-2673	2nd Int'l Conf on IW, Jan 95 participant
National Bank of Canada	UBI Project		Ratajczak	Stanley		Secure Ssytems Architect	514- 394-5000 x 5182	2nd Int'l Conf on IW, Jan 95 participant
Royal Canadian Mounted Police	Information Technology Security Section		Wolynski	Jan			613-993-8792	2nd Int'l Conf on IW, Jan 95 participant
T-Base Research and Development Inc	Security Management Integration		Breakspear	Alan		Associate Partner	613-237-5245	2nd Int'l Conf on IW, Jan 95 participant
U.K. Department of Defence	I.T. Vulnerabilites	Defence Research Agency	Corcoran	Mike			011-44-0684-894-880	

This page intentionally left blank.

This page intentionally left blank.


Public Organizations
Academia
Center for Advanced Study and Research on Intellectual Property
Center for Public Interest Law
Computer Emergency Response Team (CERT) Carnegie Mellon
TO FIRST
Computer Operations, Audit, and Security Technology (COAST)
Computer Security Research Laboratory
Computer Security Research Laboratory
Information Security Institute
Legal Information Institute
National Crime Prevention Institute
Purdue Computer Emergency Response Team (PCERT)

PUBLIC ORGANIZATIONS

ACADEMIA

Center for Advanced Study and Research on Intellectual Property (CASRIP)

University of Washington School of Law, Seattle, WA

CASRIP is an independent research and policy development institute focusing on problems in patent and other property ownership rights in the products of high technology. It aims to improve discussion and exchange of views between professionals of various countries, particularly those countries that have major intellectual property systems.

Center for Public Interest Law

University of San Diego School of Law, 5998 Alcala Park, San Diego, CA 92110-2492

This center serves as an academic center of research, learning, and advocacy in administrative law. This center also administers the Privacy Rights Clearinghouse. This Clearinghouse is funded by the Telecommunications Education Trust, a program of the California Public Utilities Commission, and its purpose is to raise consumers' awareness of how technology affects personal privacy.

Computer Emergency Response Team (CERT)

Coordination Center, Software Engineering Institute, Carnegie Mellon University,
Pittsburgh, PA 15213-3890

412/268-7090

Lucy Piccolino, Information Coordinator, 412/268-7700

The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. CERT products and services include a 24-hour technical assistance for responding to computer security incidents, products vulnerability assistance, technical documents, and seminars.

Computer Operations, Audit, and Security Technology (COAST)

Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398

This is a multiple project, multiple investigator effort in computer security research. COAST functions with close ties to researchers and engineers in major companies and government agencies. The focus of their research is on real-world needs and limitations.

Computer Security Research Laboratory

Computer Sciences Department, University of California, 2245 Engineering Unit II, Davis, CA

916/752-2149

Research in the Computer Security Research Laboratory is concerned with the development of new techniques for the design of secure systems and for demonstrating such systems to be secure. Current research activities include: (1) developing techniques for understanding malicious code and for detecting and preventing the occurrence of such code in programs, and (2) developing techniques for network intrusion detection. The intent is to flag network intruders and abusers with a low probability of false alarms. The basic philosophy is to employ rule-based approaches to detect policy violations or attempts at exploiting system vulnerabilities. A current project is developing an intrusion detection system that could be used on the INTERNET.

Information Security Institute

George Mason University, Center for Professional Development, 4400 University Drive, Fairfax, VA 22030-4440

Legal Information Institute

Cornell Law School, Myron Taylor Hall, Ithaca, NY 14853

This institute aims to explore new ways of distributing legal documents and commentary. One primary aim is the dissemination of legal information via the Internet.

National Crime Prevention Institute

University of Louisville, Belknap Campus, Brigman Hall, Louisville, KY 40292

502/852-6987

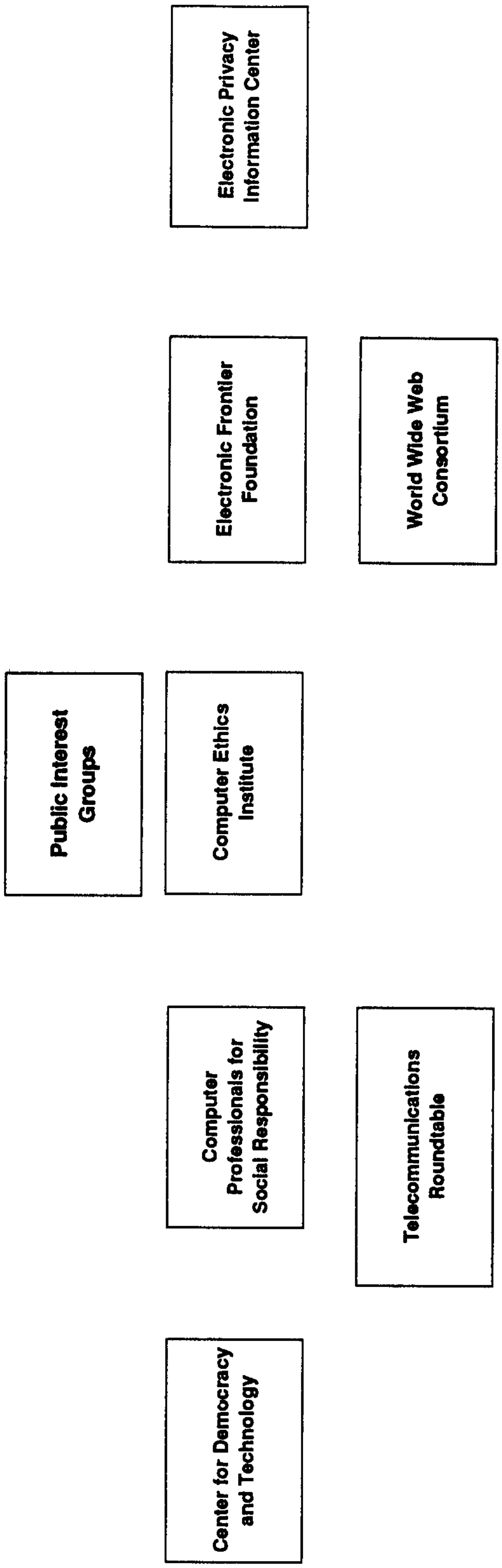
Wilbur Rykert, Director

This Institute engages in research pertaining to physical and electronic security and review of loss reduction techniques. The institute trains police officers, criminal justice planners, security personnel in the private sector and community representatives in crime prevention

Purdue Computer Emergency Response Team (PCERT)

Purdue University, Lafayette, Indiana

PCERT is a team of faculty and staff at Purdue University who work together to improve computer security, advise on policies regarding computer use and misuse, and who coordinate responses to computer security incidents on campus. The PCERT is the first university response team admitted to membership in the FIRST.


Public Interest Groups
Center for Democracy and Technology
Computer Professionals for Social Responsibility
Computer Ethics Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Telecommunications Roundtable
World Wide Web Consortium

PUBLIC ORGANIZATIONS

PUBLIC INTEREST GROUPS

Center for Democracy and Technology

Washington, DC

Jerry Berman

This is a non-profit public interest organization; its mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies. The center achieves its goals through policy development, public education, and coalition building.

Computer Professionals for Social Responsibility (CPSR)

P.O. Box 717, Palo Alto, CA 94302

415/322-3778

This is a non-profit, public interest organization concerned with the effects of computers on society. The mission of CPSR is to provide the public and policymakers with realistic assessments of the power, promise, and problems of information technology.

Electronic Frontier Foundation (EFF)

1667 K Street NW, Suite 801, Washington, DC 20006-1605

202/861-7700

The EFF is a non-profit, civil liberties, public interest organization founded in July 1990 to ensure that the principles embodied in the Constitution and the Bill of Rights are protected as new communications technologies emerge. The work of this organization focuses on protection of privacy and access to on-line resources and information.

Electronic Privacy Information Center (EPIC)

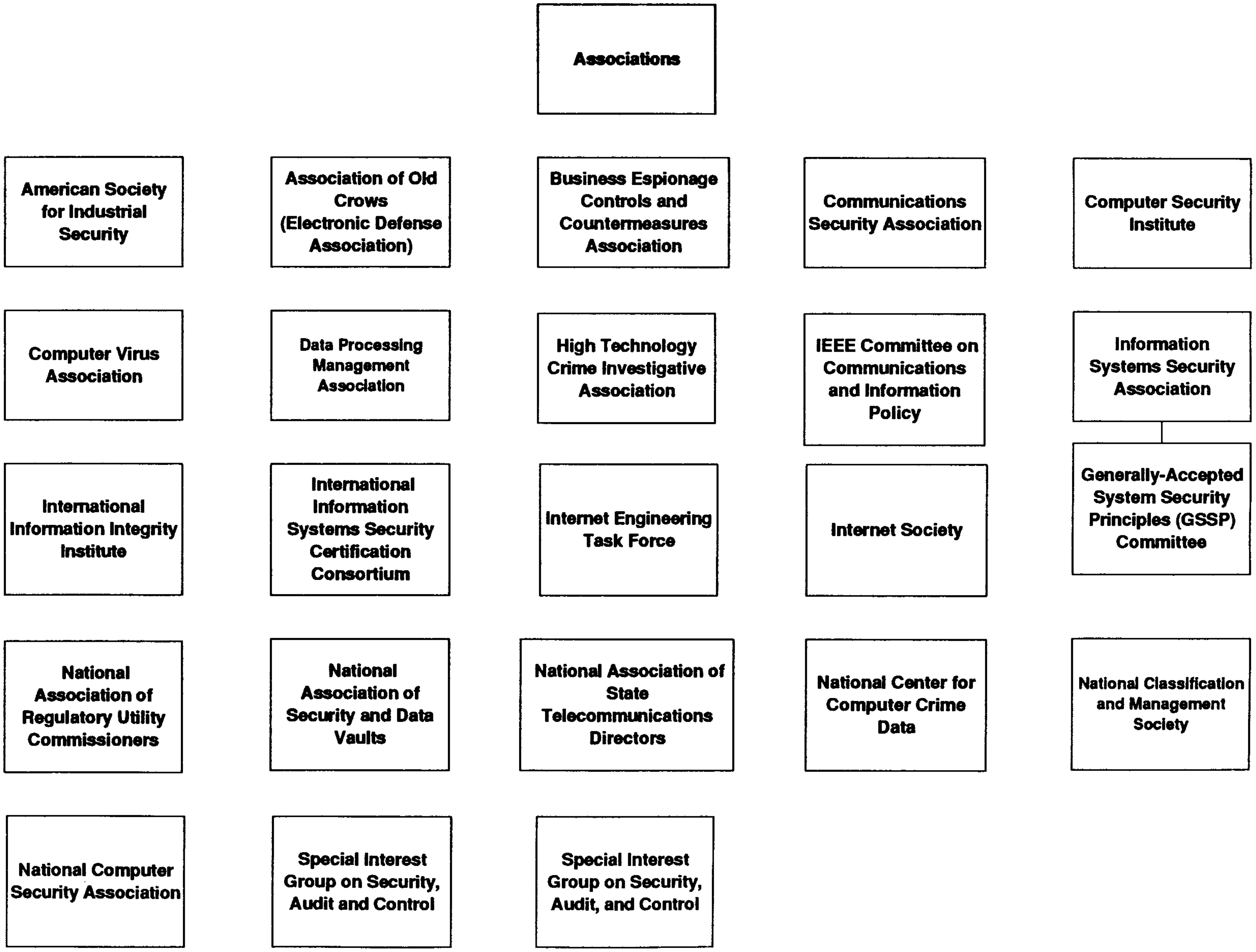
666 Pennsylvania Avenue, SE, Suite 301, Washington, DC 20003

202/544-9240

Marc Rotenburg, Director
David Sobel, Legal Counsel

This public policy group advocates for electronic privacy. It is a public interest research center, established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure (NII). It supports efforts to preserve the right of privacy in the electronic age, to give individuals greater control over personal information, and to encourage the development of new technologies that protect privacy rights. It sponsors educational and research programs, a speakers' bureau, compiles statistics, and conducts litigation. It is currently suing the NSC for details on the proposal for NSC to assume oversight of federal information security (see U.S. Security Policy Board).

This page intentionally left blank.



Associations

American Society for Industrial Security

Association of Old Crows (Electronic Defense Association)

Business Espionage Controls and Countermeasures Association

Communications Security Association

Computer Security Institute

Computer Virus Association

Data Processing Management Association

High Technology Crime Investigative Association

IEEE Committee on Communications and Information Policy

Information Systems Security Association

International Information Integrity Institute

International Information Systems Security Certification Consortium

Internet Engineering Task Force

Internet Society

Generally-Accepted System Security Principles (GSSP) Committee

National Association of Regulatory Utility Commissioners

National Association of Security and Data Vaults

National Association of State Telecommunications Directors

National Center for Computer Crime Data

National Classification and Management Society

National Computer Security Association

Special Interest Group on Security, Audit and Control

Special Interest Group on Security, Audit, and Control

PRIVATE ORGANIZATIONS

ASSOCIATIONS

American Society for Industrial Security

1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209

703/522-5800

Michael Stack, Executive Director; F. Joseph Ricci, Director of Marketing

This organization acts as a conduit for security professionals; it provides programs and resources at all local, national, and international levels which enable members to update and exchange information and expertise. The role of ASIS Standing Committees and Councils is to keep members informed of the latest developments in security practice and technology and to further integrate specialized knowledge and skills. The ASIS has 27 standing committees, 6 subcommittees, and 3 councils.

- Computer Security Committee: John Spain, Chairman. 404/614-4141.
- Disaster Management Committee: Robert Lee, Chairman. 818/775-4099.
- Government Security Committee: Cynthia Conlon, Chairman. 310/393-0411 X7201.
- Telecommunications Committee: Robert Postovit, Chairman. 206/345-7351.
- Terrorist Activities Committee: Robert Disney, Chairman. 718/481-6400.
- White Collar Crime Committee: Frederick Verinder, Chairman. 202/324-4805.

Association of Old Crows (Formerly the Electronic Defense Association)

1000 N. Payne St., Alexandria, VA 22314

703/549-1600

Gus Slayton, Director

This is a professional association of scientists, engineers, managers, operators, educators, military personnel and others engaged in the science of electronic warfare and related areas. Approximately 23000 members in 92 regional groups.

Business Espionage Controls and Countermeasures Associations

P.O. Box 55582, Seattle, WA 98155

206/364-4672

William Johnson, Executive Director

This association has management consultants, law enforcement officials, and information specialists involved in business espionage controls and countermeasures. Promotes business awareness of the growing concern of espionage in the business community. It publishes "The Business Espionage Report" monthly.

Communications Fraud Control Association

1990 M Street, NW, Suite 508, Washington, DC 20036

202/296-3225

Frances Feld, Executive Director

The thrust of the Association is to find effective ways to combat the growing problem of communications fraud. The Association has the following missions:

- serves as a clearinghouse for telecommunications fraud information
- develops training programs on the latest anti-fraud technologies
- supports legislative protection
- improve investigative standards and techniques

Membership includes representatives from MCI, AT&T, SBS, ITT, Network One, many of the Bell Operating Companies and smaller resellers of telecommunications services.
Membership categories include PBX owners, Corporate end-users (Dupont, J.C. Penny, hospitals and universities), International PTTs, Operator Service Providers, Independent Public Payphone Providers, Secret Service and FBI agents, local and Canadian provincial authorities, prosecutors and telecommunication consultants.

Computer Security Institute

600 Harrison Street, San Francisco, CA 94107

415/905-2370

Patrice Rapalus, Director

Provides computer and information security professionals with information resources and support through membership, training, conferences and networking opportunities. Membership includes many major American Corporations: Aetna Life & Casualty, Allstate Insurance, AT&T, Blue Cross, Boeing Information Services, Chase Manhattan Bank, Coca-Cola Company, Dean Wittier, Dow Chemical, Dupont, Eastman Kodak, Exxon, etc.

Computer Virus Association

408/727-4559

John McAfee, Chairman

This association offers assistance to companies involved in identifying and eradicating computer viruses. It conducts research programs and compiles statistics. Approximately 60 members.

Data Processing Management Association

505 Busse Highway, Park Ridge, IL 60068

708/825-8124

Suzanne Lattimore is the POC

Membership is made up of managerial personnel, staff, educators, and individuals interested in management of information resources. It maintains a Legislative Communications Network, professional education programs, and sponsors student organizations around the country. Membership numbers 24000 in 12 regional groups and 275 local groups.

Forum of Incident Response and Security Teams (FIRST)

National Institute of Standards and Technology, A-216 Technology. Gaithersburg, MD 20899

301/975-3359

FIRST is an international consortium which brings together a variety of computer security incident response teams from government, commercial, and academic organizations. It aims to foster cooperation and coordination in incident prevention, to provide members with technical information, tools, methods, assistance, and guidance, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

High Technology Crime Investigative Association (HTCIA)

P.O. Box 162034, Sacramento, CA 95816

916/441-1333

The HTCIA encourages, promotes, aids and effects the voluntary interchange of data, information, experience, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Information Systems Security Association, Inc.

800 N. Lingbergh, G2EE, St. Louis, MO 63167

314/694-7661

Ms. Genevieve M. Burns (of Monsanto Corp.), President

This is an international organization providing educational forums, publications and peer interaction opportunities. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

Membership: greater than 2,000. Includes major U.S. and international corporations, leading consulting firms, government agencies, and educational institutions. Has more than 35 chapters in major American cities.

International Information Integrity Institute (I4)

333 Ravenswood Avenue, Menlo Park, CA 94025

415/859-4771

Dr. Bruce Baker, Program Manager, SRI International

Assists major enterprises and government agencies in protecting their information assets; I4 is dedicated to advancing information security and enterprise protection by encouraging prudent management responsibilities that lead to a standard of due care.

Internet Engineering Task Force (IETF)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA

703/620-8990

G. Malkin, IETF Secretariat

The IETF is the protocol engineering and development arm of the Internet. It is a large, self-organized, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual but there isn't any membership in the IETF. Actual technical work of the IETF is done in its working groups (routing, network management, and security). The mission of the IETF includes: (1) identifying and proposing solutions to pressing operational and technical problems in the Internet, (2) specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet, (3) making recommendations to the Internet Engineering Steering Group (IESG), (4) facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community, and (5) providing a forum for the exchange of information within the Internet community.

Internet Society

12020 Sunrise Valley Drive, Suite 270, Reston, VA 22091

703/648-9888

Vinton G. Serf, President

A nongovernmental, international organization for global cooperation and coordination for the Internet and its technologies and applications. Principal purpose is to maintain and extend the development and availability of the Internet and its associated technologies and applications.

National Association of Security and Data Vaults

716 E. Washington Str., Syracuse, NY 13210

315/475-7743

Ellie Seitz, President

This association has individuals and firms in the private security vault and data storage business. Its accredited members are vault businesses that have met standards set forth by the association. It promotes establishment of non-bank, high-security centers for data storage operations. The association has about 80 members.

National Center for Computer Crime Data

1222 17th Ave., Suite B, Santa Cruz, CA 95062

408/475-4457

Jay J. Bloombecker, Director

This organization is made up of individuals and organizations in the security, law enforcement, legal, business, accounting, and computing professions. It facilitates the prevention, investigation, and prosecution of computer crime by disseminating documents and other data to those in need of such information.

National Classification and Management Society

6118 Roseland Drive, Rockville, MD 20852

301/231-9191

Eugene J. Suto, Executive Secretary

This society manages, supervises, and performs in a security classification management capacity in industry, government, the military services, and educational institutions. The society seeks to establish systems and techniques for identifying information or materials requiring protection in the national interest; it also helps establish procedures and practices for management of classified materials. The society has about 2300 members in 29 local groups.

National Computer Security Association

10 South Courthouse Avenue, Carlisle, PA 17013

717/258-1816

Robert Bales, Executive Officer. Paul Gates, Membership Director

This is a membership organization which provides educational materials, training, testing, and consulting services to improve computer and information security, reliability and ethics.

Special Interest Group on Operating Systems, Association for Computing Machinery

University of Washington, Department of Computer Sciences, FR-35, Seattle, WA 98195

208/543-9204

Henry Levy, Chairman

A special interest group of the Association for Computing Machinery. The group is made up of individuals interested in reliability, integrity and security of data, computer operating systems, communications among computing processes, and much more. Approximately 8100 members.

Special Interest Group on Security, Audit and Control

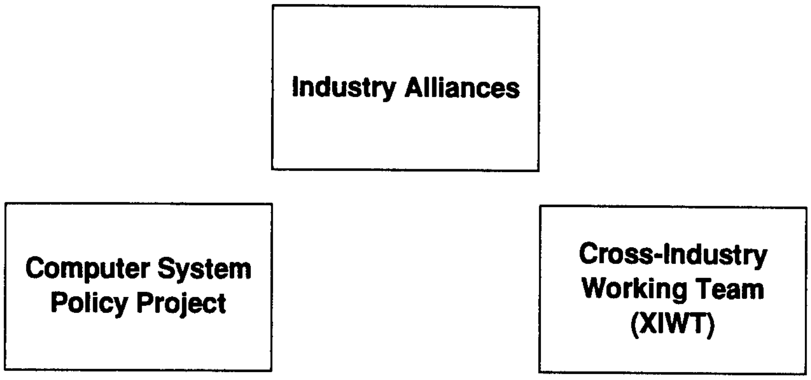
Association for Computing Machinery, 1515 Broadway, New York, NY 10036

212/869-7440

Daniel Faigin, Chairman

A special interest group of the Association for Computing Machinery. The groups is made up of information processing security personnel, auditors, accountants and computer technicians. Its purpose is to maintain high levels of skill and awareness regarding technology and practice in the fields of computer security, audit, and control. Approximately 1300 members.

This page intentionally left blank.



Industry Alliances

Computer System Policy Project

Cross-Industry Working Team (XIWT)

PRIVATE ORGANIZATIONS

INDUSTRY ALLIANCES

Cross-Industry Working Team (XIWT)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100,
Reston, VA, 22091

703/620-8990

Charles N. Brownstein, Executive Director

XIWT is a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful and sustainable national information infrastructure (NII). It aims to foster understanding, development and application of technologies that cross industry boundaries, to facilitate the conversion of the NII vision into real-world implementations, and to facilitate a dialogue among representatives of stakeholders in the private and public sectors.

Computer Systems Policy Project

c/o Pam Fandel, Computer System Policy Project, 1735 New York Avenue, NW,
Suite 500, Washington, DC 20006

202/662-8403

The Computer Systems Policy Project (CSPP) is an affiliation of chief executive officers of American computer companies that develop, build, and market information processing systems and software. CSPP's members include the chief executives of Apple, AT&T, Compaq, Control Data Systems, Cray Research, Data General, Digital Equipment, Hewlett-Packard, IBM, Silicon Graphics, Sun Microsystems, Tandem, and Unisys. Upon forming CSPP in 1989, the CEOs made a commitment to work together to develop and personally advocate public policy positions on trade and technology issues that affect their industry, all high-technology industries, and hence, the nation. To date, CSPP has issued numerous reports which outlines the CEO's positions on a variety of issues.

This page intentionally left blank.

National
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
American Bankers Association			Daguia	Kawika				
Arnold & Porter			Smith	Jeffrey	H	Attorney		
AT&T			Lawler	Dan				
BDM			Mylan	John				Source - SIWS
Bellcore			Leary	Bruce		Director of Corporate Computer and Network Security		
Bolt, Beranek and Newman Inc (BBN).	Security Technology Communications Division		Kent	Stephen		Chief Scientist		
Booze-Allen, Hamilton Corporation (BAH)			Gergley					Source - SIWS
Booze-Allen, Hamilton Corporation (BAH)			Herman	Mark				Source - SIWS, War Gaming and IW
Carnegie Mellon University	Research and Development		Longstaff	Thomas		Manager		Quoted in Wash Post article, Jan 24 95
Center for Strategic and International Studies			Snider	Don	M.	Director, Political-Military Studies	202/775-3278	Source - SIWS
Chronicle of Higher Education			Wilson	David		Investigative Reporter		Follows computer security issues; Quoted in Wash Post article, Jan 25 95
Citibank Corp	Corporate Audit		Philhower	William		Vice-President	212/657-8937	
COMPAQ Computer Corporation	Strategic Technology		Angelo	Michael	F	Senior Member, Technical Staff	713/374-8141	Security Working Group, Cross Industry Working Team
Computer Sciences Corporation (CSC)	Information Security		Gulick	John			410/641-2588	
Computer Sciences Corporation (CSC)	Information Security		Harper	Jim				
Computer Sciences Corporation (CSC)			Lackey	Bill			310/615-0311	
Computer Sciences Corporation (CSC)			Rhodes	Mary			310/615-0311	
Computers, Freedom, and Privacy			Koball	Bruce				Public interest group holds an annual conference to discuss computer legal issues. Attended by hackers, civil libertarians, law enforcement, and gov't.
Computerworld			Anthes	Gary	H	Senior Editor	202/347-0134	
Connecticut Mutual			Bell	David		Information Security Officer		
Counter Technology, Inc.	Field Operations		Kerns	John	M	Director		
Electronic Frontier Foundation			Gilmore	John		Co-Founder		
Ernst & Young			White	Dan		National Director of Information Security		
Harris	RF Communications Division		Massari	Chester	A	VP of Operations		Tac/Strat comm sys & info security; tech transfer; Def Electronics article, Aug 94.
Harvard University	Program on Information Resources Policy	Center for Info Policy Research	Oettinger	Tony	G.	Chairman	617/495-4114	Source - SIWS
Integrated Risk Management Group			Ozier	Will		President	707/762-2227	
Intel Corporation	Mobile Technology Lab	Intel Architecture Labs	Aucsmith	David		Security Architect	503/264-5562	Acting Chairman, Security Working Group, Cross Industry Working Team
Winn Schwartau Interpact, Inc.	Information Security and Warfare		Schwartau	Winn		Executive Director	813-393-6600	
Internet Society			Cerf	Vincent		President	703-648-9888	
Internet Society			Rutkowski	Tony		Executive Director		

National
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Meyer, Hendricks, Victor, Osborn & Maledon, P. A.			Lechter	Michael	A			Lawyer w/ 20 yrs experience in intellectual property law. Conversant in electronic signatures. Contributes to Wash Technology.
MIS Training Institute	Information Security Institute		Cutler	Ken		VP	508/879-7999	
Motorola, Inc.	Government and Systems Technology Group		Foster	Robert	I	Director and VP, Technical Staff		
National Computer Security Association (NCSA)			Bales	Robert		Executive Director	717/258-1816	
National Computer Security Association (NCSA)			Cobb	Stephen		Technology Analyst	717/258-1816	
National Computer Security Association (NCSA)			Gates	Paul		Membership Chairman	717/258-1816	
National Computer Security Association (NCSA)			Kabay	M.	E.	Director of Education		Internet Engineering Society Security Working Group
North American Electric Reliability Council			Gorzelnik	Gene				
Northwest Airlines Corp	Information Security Division		Carlson	Carl		Data Security Manager		
Owens-Corning	Information Security		Hertsch	Jan		Manager		
Private Consultant			Rona	Thomas		Dr.		Former Dep Dir, OSTP
Private Consultant			Strassmann	Paul				Former Director of Defense Information, OASD(C3I)
Quest Tech			Nelson	Andy				Source - SIWS
QuesTech Inc.	Applied Engineering Group		Hogler	James		Senior Engineer	703/349-7234	
SAIC			Andrews	Duane		Corporate VP		Former ASD(C3I)
SAIC			Knecht	Ron			703/749-8779	IW; INFOSEC, Former OASD (C3I)
SAIC			Kraus	George		Senior Analyst	734-5597	panel member IW track AFCEA ACCE 95; OSD(Policy); intelligence, net assessment
SAIC			McKitrick	Jeff				Source - SIWS
SAIC			Rankin	Bob	W		703/556-7008	IW, legal and regulatory
SAIC			Rasch	Mark	D	Esq.	703/917-5430	Lawyer; Former U.S. Attorney's Office; Specializes in computer/Internet crime.
SAIC			Snell	Steve			410/691-5577	IW; INFOSEC; policy
SAIC			Winkler	Ira			410/266-0993	IW; emerging technology
SAIC			Ziegler	Bernie		Program Manager	703/790-7452	IW PM; Organizations
SAIC - Canada			Whalen	Sue		Computer Scientist	613/563-2122	
San Diego Super Computer Center			Shimomura	Tsutomu				
Silicon Graphics Inc. (Formerly)			Farmer	Dan				Wrote COPS and SATAN computer and network security analysis software which is distributed freely on Internet. Carnegie CERT alumnus.
Trusted Information Systems			Avolio	Fred		Product Manager		
U S West Technologies, Inc.			O'Toole	Kevin		Member Technical Staff	303/541-6966	Security Working Group, Cross Industry Working Team
University of Vermont	Political Science		Devost	Matthew	G	Graduate Student	802/656-3050	2nd Int'l Conf on IW, Jan 95 participant
USA Group, Inc.			Hepker	Ed		Administrator of Info Security		Indianapolis; quoted in Computerworld, Nov 94 article
Vector Research, Inc.			Otis	Glenn				Source - SIWS
Whole Earth Lectronic Link (WELL)			Katz	Bruce		CEO		WELL provides Internet access and on-line discussions. Katz helped FBI apprehend Mitnick in Feb 95.
Williams, Brinks, Olds, Gibson and Lione			Cook	William	J			
Electronic Frontier Foundation			Kapor	Mitchell		Chairman	202-347-5400	
Computer Professionals for Social Responsibility			Kells	Kathleen		Managing Director	415-322-3778	

State and Local
Points of Contact

Organization	Sub Organization	Sub Organization	Last Name	First	MI	Title	Telephone	Remarks
Ohio Supercomputer Center	ECLIPS		Ritter	Jeffrey	B	Program Director	614/292-5691	Lawyer; 2nd Int'l Conf on IW, Jan 95 participant
Texas Department of Transportation	Division of Automation		Tompkins	Williams		Information Security Manager		Rec'd CSI "Security Program of the Year" in 1994. Previous winners were CSX Technology in 1993 and Martin Marietta in 1992.

This page intentionally left blank.

APPENDIX B

UNITED STATES CODE
ANNOTATED BIBLIOGRAPHY AND INDEX

The following is an annotated bibliography of U.S. statutes applicable to Information Warfare and Information Assurance. The abstracts identify the general purpose of the statute and any assigned responsibilities. Key words are also provided. An "Index to Relevant Topics" follows the annotated bibliographies.

Arms Export Control Act of 1968.

KEY WORDS: cryptographic, TEMPEST, export, DoS

ABSTRACT: Export license from the Department of State is required to export cryptographic or TEMPEST information.

Automatic Data Processing Equipment Act of 1965, Public Law 89-306, (Brooks Act).

KEY WORDS: GSA, Brooks Act, IT procurement, acquisition

ABSTRACT: The Brooks Act amended the Federal Property and Administrative Services Act (FPAS) of 1949. FPAS had previously created the General Services Administration (GSA). The Brooks Act confers upon GSA government-wide responsibility for the economic and efficient acquisition of information technology, including 'sole procurement authority'. In practice, GSA delegates this authority to the agencies. The act implemented a government wide procurement policy promoting competitive bidding, centralized procurement of information technology systems under GSA and established GSA's Board of Contract Appeals. The act assigned responsibilities to the Office of Management and Budget, the Department of Commerce, the National Bureau of Standards (predecessor to National Institute of Standards and Technology) and the General Services Administration for Federal IT procurement. The Paperwork Reduction Act expanded these IT roles. The Computer Security Act specifically assigned information security roles to the Department of Commerce, NIST and GSA and secretaries of Federal departments. With the departure Representative Brooks from Congress, the Brooks Act is a prime target for the 104th Congress as they seek to streamline IT procurement. It is not expected, however, that changes to IT procurement will dramatically change responsibilities for information systems security.

Cable Communications Policy Act of 1984.

KEY WORDS: cable television, privacy

ABSTRACT: Limits cable television companies in the use of subscriber personal information.

Chief Financial Officers Act of 1990, Public Law 101-576, November 15, 1990.

KEY WORDS: OMB, Federal government, financial management

ABSTRACT: This act enhances the functions of the Office of Management and Budget in order to improve the efficiency and effectiveness of the Federal government. It establishes an Office of Financial Management in OMB and requires a Chief Financial Officer in each Executive agency. Agencies will submit five year financial management plans and status reports and will establish accounting internal controls that provide complete disclosure of agency financial activities.

Communications Act of 1934, Public Law 73-416, June 19, 1934.

KEY WORDS: Commercial carriers, FCC, war powers, NCS

ABSTRACT: Revision of the Radio Act of 1927. The purpose of the Communications Act of 1934 was to regulate interstate and foreign communications by wire and radio in the public interest. It established the Federal Communications Commission and addressed radio stations operated by foreign governments, willful or malicious interference with radio transmissions, and assigned war powers to the President. The Secretary of Commerce will serve as the President's principal adviser on telecommunications policies pertaining to the Nations economic and technological advancement. The Secretary of Commerce will also advise the Director of the Office of Management and Budget relating to the procurement and management of Federal telecommunications systems. The Secretary will also develop policies which relate to international telecommunications issues in coordination with the Secretary of State and other interested agencies. Amendments to the act since 1934 have been generally narrow in focus and scope.

Communications Assistance for Law Enforcement Act of 1994, Public Law 103-414, October 25, 1994 (Digital Telephony Act).

KEY WORDS: Intercept, wiretap, carriers

ABSTRACT: "A telecommunications carrier shall ensure that its equipment, facilities, or services...are capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment [and] to access call-identifying information." Excludes data carriers and on-line services. This act also amended the Electronic Communications Act of 1986 to include cordless telephones and certain data communications transmitted over radio. It also clarified fraudulent alteration of commercial mobile radio instruments.

Communications Satellite Act of 1962.

KEY WORDS: FCC, regulatory, satellite

ABSTRACT: This act expanded FCC regulatory jurisdiction assigned by the Communications Act of 1934.

Computer Fraud and Abuse Act of 1986, Public Law 99-474, October 16, 1986.

KEY WORDS: Computer crime, Federal employees, Federal computer systems

ABSTRACT: Made computer fraud or theft across state lines a Federal crime. Also excluded Federal employees from the provisions of Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. It remained a misdemeanor for non-Federal employees to access, use, modify, destroy, or disclose information from a Federal computer. It was feared that Federal employees might be prosecuted for accidental damage or disclosure or whistle blowing.

Computer Matching and Privacy Act of 1988.

KEY WORDS: Privacy, computer matching, Federal government

ABSTRACT: Protects privacy associated with computer matching capabilities and practices of the Federal government. Disclosure and purposes of computer matching are restricted and reporting requirements are levied.

Computer Security Act of 1987, Public Law 100-235, January 8, 1988.

KEY WORDS: NSA, NIST, NSTISSC, CSSPAB, law, sensitive information, classified information, computer security

ABSTRACT: The Computer Security Act assigns responsibilities for the security of sensitive Federal information. NIST is responsible for policy for unclassified-but-sensitive information and is to develop guidance and standards for encryption of data. NIST can, upon request, assist the private sector. NSA is responsible for providing technical assistance to NIST. The act established the

National Computer System Security and Privacy Advisory Board (CSSPAB). CSSPAB is a twelve member advisory group of recognized experts in computer and telecommunications systems security and technology. The CSSPAB advises the Secretary of Commerce and Director, NIST. The CSSPAB's mission is to identify issues relative to computer systems security and privacy. The Board focus is limited Federal unclassified systems. The act specifically excludes private sector and Federal classified and Warner Exempt systems. Each Federal agency is to provide mandatory computer security awareness training.

Constitution of the United States, Fourth Amendment, (Bill of Rights), Ratified December 15, 1791.

KEY WORDS: Privacy, unreasonable search, seizure, warrants

ABSTRACT: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Public Law 98-473

KEY WORDS: Computer crime, Federal computers, espionage, computer passwords

ABSTRACT: First computer crime legislation. This statute defined computers, excluding electronic typewriters and hand calculators and addressed the unauthorized access of computer systems making it a felony to access Federal computers to obtain classified information with the intent to do harm to the U.S. or benefit a foreign country. It also made it a misdemeanor to access any Federal computer without authorization. Civil damage suits were authorized against illegal wiretappers. A 1986 amendment made trafficking in stolen computer passwords a criminal act. Under authority of this act, the U.S. Attorney's Office, the FBI and Secret Service engaged in cooperative efforts aimed at computer crime.

Department of Defense Authorization Act of 1982, Public Law 97-86 (Warner Amendment)

KEY WORDS: DoD IT procurement, GSA, Brooks Act, C3I, cryptographic

ABSTRACT: Exempted DoD procurements from the Brooks Act if they involved intelligence, cryptographic, command and control, embedded electronics in a weapon system, or equipment critical to a military or intelligence mission.

Domestic Wiretap Act of 1968 (Federal Wiretap Law).

KEY WORDS: FCC, wiretap, monitoring, consent, e-mail

ABSTRACT: Expanded in 1986 to include computers and electronic mail. Permits monitoring if only one party consents. FCC and some state laws require two-party consent. Violation of FCC regulation is a tariff violation only. Originally FCC required a warning tone but subsequently rescinded that requirement. For government employees, "consent" is more loosely defined. Agency policy and/or stickers on telephone instruments or banners on computer screens during log-on can be considered adequate for "consent."

Electronic Communications Privacy Act of 1986, Public Law 99-508, October 21, 1986.

KEY WORDS: Privacy, wiretap, interception, wire, oral, cellular, cordless, data communications

ABSTRACT: Updated Federal privacy clause in Omnibus Crime Control and Safe Streets Act of 1968 to include digitized voice, data, or video whether transmitted over wire, microwave, or fiber optics. The act applies to transmissions regardless whether they are carried by common or other carriers. Included transmissions where users had an expectation of privacy. Cellular phones were included but cordless were not. The Communications Assistance for Law Enforcement Act of 1994 (Digital Telephony Act) added cordless phones and specified certain data communications transmitted over radio. Warrants are now required for interception of cordless phone conversations. Court warrants, based on probable cause, are required to intercept wire or oral communications. Exceptions to the warrant requirement are: telephone companies and the FCC, police officers when they are a party to the call, and with the consent of one party.

Electronic Funds Transfer Act of 1980.

KEY WORDS: EC/EDI, electronic funds transfer

ABSTRACT: Addresses the privacy of electronic funds transfer. Specifies the responsibilities of financial institutions including a requirement that financial institutions notify customers of the circumstances surrounding third party access to electronic financial information in the course of normal business operations.

Export Administration Act of 1979, Public Law 96-72, September 29, 1979.

KEY WORDS: DoC, export, scientific data, technical data

ABSTRACT: Export of scientific and technical data only authorized with an export license from the Department of Commerce. See also Arms Export Control Act of 1968 for Department of State responsibilities.

Fair Credit Reporting Act of 1970, Public Law 91-508.

KEY WORDS: credit reports, consumer credit

ABSTRACT: Intended to protect the privacy of individuals, the Fair Credit Reporting Act covers consumer credit reports. It details legal uses of credit reports, prohibiting the inclusion of obsolete information and identifies information that must be provided to the U.S. government. It also specifies the process by which a consumer can obtain his credit report and challenge information.

Federal Managers Financial Integrity Act of 1982, Public Law 97-255.

KEY WORDS: Internal controls, NPR, CSSPAB, OMB, GAO, computer security

ABSTRACT: The act amended the Budget and Accounting Act of 1950 to require the GAO to develop internal accounting and administrative standards and OMB to establish guidelines for Executive agencies to conduct annual evaluations of their internal accounting and administrative controls. Annual statements are submitted to the President and Congress. Both the National Performance Review (NPR) and the CSSPAB recommend linking computer security oversight to the oversight required by this act.

Foreign Intelligence Surveillance Act of 1978, Public Law 95-511, October 25, 1978.

KEY WORDS: Foreign intelligence, wiretap, time of war, electronic surveillance, Senate Select Committee on Intelligence

ABSTRACT: The President, through the Attorney General, may, without court order, authorize wiretaps, for up to one year, to gather foreign intelligence subject to certain restrictions. The Attorney General must submit a written oath to a special seven member court established by this act and report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. The Attorney General may direct communications carriers to support this effort. Other Federal officers must request a court order. Requests must include certifications by the Assistant to the

President for National Security Affairs or other executive branch official responsible for national security or defense. During time of war, the President, through the Attorney General, may authorize electronic surveillance without a court order for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

Freedom of Information Acts of 1966 (1969, 1970, 1989), Public Law 93-502.

KEY WORDS: FOIA, national security

ABSTRACT: Companion law to the Privacy Act requiring agencies of the Federal government to release information to citizens. Agencies can refuse to release information related to national security or foreign relations but if challenged in court must prove why the information should not be released.

Government Performance and Results Act of 1993.

KEY WORDS: Strategic planning, performance planning, results

ABSTRACT: Purpose of this act is to systematically hold Federal agencies accountable for achieving program results; improving program effectiveness by focusing on results, service, quality, and customer satisfaction. The act requires Executive agencies, except CIA, USPS, GAO, and others, to draft Strategic Plans no later than September 30, 1997. Special planning and reporting requirements are levied on the USPS. Plans will include relationship between performance goals and general goals and will cover a five year period and be updated every three years. Agencies will also draft annual performance plans covering each program activity in the budget; establishing objective, quantifiable, and measurable performance goals. By March 31, 2000, agencies prepare annual program performance reports; comparing actual performance for against Performance Plans. OMB is the proponent for this act and will identify agencies to participate in pilot projects. OPM will develop manager training. GAO will report to Congress no later than June 1, 1997 on pilot projects and likelihood of other Federal agency compliance.

Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351.

KEY WORDS: Privacy, wire, oral

ABSTRACT: This act addresses the privacy of wire and oral communications. It specifies the conditions under which an authorized agency may intercept private communications. It was updated by the Electronic Communications Privacy Act of 1986 (P.L. 99-508) in light of new technology.

Paperwork Reduction Act of 1980, Public Law 96-511, December 11, 1980.

KEY WORDS: OMB, IRM, oversight, e-mail, imaging

ABSTRACT: "The principal information resources management (IRM) statute for the Federal government. It created the Office of Information and Regulatory Affairs (OIRA) in OMB to establish government-wide IRM policies and oversee and review agency implementation. The act specifically requires agency [sic] to acquire/use IT to improve service delivery and program management, increase productivity, enhance the quality of decision-making, reduce fraud and waste. It also requires that agencies develop a 5-year plan for meeting the agency's IT needs and that the agency head designate a senior IRM official (who reports directly to the agency head) to carry out agency IRM responsibilities under the act."[OMB, 1995] The act also made OMB responsible for improving Federal government administrative efficiency through the use of new technologies such as electronic mail and electronic document storage (imaging). These responsibilities, which complement those in the Communications Security Act of 1934, give OMB an oversight role in information security.

Posse Comitatus Act of 1878, 18 USC 1385, June 18, 1878.

KEY WORDS: Law enforcement, Federal troops

ABSTRACT: The Posse Comitatus Act prohibits the use of the Army and Air Force as posse comitatus. Though not proscribed, the use of the Navy is also generally prohibited by Navy instruction. The Coast Guard is excluded and the Navy may be given permission to assist the Coast Guard. Collaboration of military law enforcement with agents of the Federal, state, and local agencies has generally been found not to violate the act as long as the military role is passive and so long as they never exercise regulatory, proscriptive, or compulsory military in the execution of civilian law enforcement.

Privacy Act of 1974, Public Law 93-579, December 31, 1974.

KEY WORDS: Privacy, access, civil damages, security

ABSTRACT: The objective of the Privacy Act of 1974 is to protect personal privacy from invasions by Federal agencies, in light of increasing use of information technology in the Federal government and the associated increase in personal information maintained by Federal agencies. The law allows individuals to specify what information may be held by a government agency and gives individuals the right to obtain information held on them by the Federal government. The act specifies physical security practices, information management practices, and computer and network controls necessary to ensure individual privacy. It also levied civil and criminal penalties for violations of the provisions of the act.

Right to Financial Privacy Act of 1978

KEY WORDS: Privacy, financial, investigators

ABSTRACT: The Financial Privacy Act requires investigators to present "formal written requests" to review the financial records on an individual held by a financial institution. Investigators must simultaneously notify the individual.

Semiconductor Chip Protection Act of 1984, Public Law 98-620, November 8, 1984.

KEY WORDS: Intellectual property, copyright, computer chips, mask work

ABSTRACT: This act extends copyright protection for 10 years to the owner/creator of the mask work contained in a semiconductor chip. Protection extends from the day the work is registered or commercially exploited anywhere in the world. The President, by proclamation, extend equal protection to foreign nationals if the nation recognizes equal protection to U.S. nationals.

Violent Crime Control and Law Enforcement Act of 1994, Public Law 103-322, September 13, 1994 (Crime Bill of 1994; Computer Abuse Amendments Act of 1994).

KEY WORDS: Computer Fraud and Abuse Act, financial systems, Federal computer laws

ABSTRACT: Section 29000 of this act is cited as the Computer Abuse Amendments Act of 1994. This act changes Federal computer crime to specifically define illegal activity on computers used in interstate commerce or communications. It also treats damage by unauthorized and authorized--insiders vs. trespassers--equally. Through an oversight, the act deleted language in the Computer Fraud and Abuse Act of 1986 which protected Federal and financial computer systems from unauthorized access, alteration or damage. The 104th Congress is expected to correct this oversight. Both acts exclude computers used in foreign commerce. The act also makes intentional damage of a computer system or information a felony but accidental or reckless damage remains a misdemeanor. Some in the information warfare community view this as a decriminalization of hacking.

U.S. CODE
INDEX TO RELEVANT TOPICS

Title	Section	Description
5	552	**Privacy Act of 1974**
5	552	Access to and disclosure of ADP records on individuals
5	552	**Freedom of Information Act of 1966, 1969, 1970, 1989**
5	552	Federal agencies may not sell or rent mailing lists
8	1182	Any foreigner may request a list from the INS automated listing of undesirable visitors. DoS and DoJ must publish guidelines for updating list.
10	2315	National security systems
12	3401	**Right to Financial Privacy Act of 1978**
15	271-278	**National Bureau of Standards Act of 1901**
15	1052	Trademark registration (Lanham Act)
15	1681	**Fair Credit Reporting Act of 1970**
15	1693	**Electronic Funds Transfer Act of 1980**
15	1802	Carriers furnishing information necessary to accomplish electronic surveillance
18	105	Sabotage
18	644	Embezzlement of public money by bank employees
18	793	Gathering information about U.S. communications facilities or defense information for a foreign power
18	1029	**Credit Card Fraud Act**
18	1029	Fraudulent use of credit cards, passwords, or telephone access codes
18	1030	**Counterfeit Access Device and Computer Fraud and Abuse Act, 1984**
18	1030	**Computer Fraud and Abuse Act of 1986**
18	1343	Wire fraud using interstate communications systems
18	1362	Civil defense functions of U.S., malicious injury to government property
18	1385	**Posse Comitatus Act of 1878**
18	2071	Concealment, removal or mutilation of public records
18	2319	Criminal infringement of copyright
18	2510	**Electronic Communications Privacy Act of 1986**
18	2510	**Omnibus Crime Control and Safe Streets Act of 1968**
18	2510	Interception of wire, oral, or electronic communications
18	2510	Electronic communications, defined
18	2510	Electronic storage, defined
18	2510	Oral communications, defined
18	2510	Wire communications, defined
18	2511	Intentional interception and disclosure of content, criminal
18	2511	Electronic surveillance of foreign intelligence by U.S. government, limitations

Title	Section	Description
18	2511	Radio interceptions; permissible
18	2511	Authorization for electronic surveillance to determine existence and capability of equipment of non-authorized persons; excepted conduct
18	2511	Consent to COMSEC monitoring
18	2512	Prohibitions against assembly of electronic intercept devices
18	2512	Contract for manufacturing or distribution of intercepting devices
18	2516	Interception of Wire, Oral, or Electronic communications
18	2516	**Atomic Energy Act of 1954**
18	2516	Interception of currency transactions
18	2516	Military assistance and sales; arms exports
18	2517	Privileged communications
18	2518	Emergency interception; application
18	2701	Unauthorized access to electronic information
18	2702	Stored wire and electronic communications and transactional records access; disclosure of contents
18	2703	Stored wire and electronic communications and transactional records access; Government access
18	2709	Stored wire and electronic communications and transactional records access; Foreign powers
18	2710	Stored wire and electronic communications and transactional records access; definitions
18	2778	Export of software or data controlled by DoD
19	482	Customs officers may stop/search with reasonable cause merchandise was imported against law or w/o paying duty tax
22	2751 et seq.	**Arms Export Control Act of 1968**
22	2751 et seq.	Export of cryptographic and TEMPEST information
26	408	Social security numbers
26	6103	Tax Records
29	2001	**Employee Polygraph Protection Act of 1988**
31	3512	**Chief Financial Officers Act**
31	3512	**Federal Managers Financial Integrity Act**
35	181 et seq.	**Invention Secrecy Act of 1951**
40	759	**Computer Security Act of 1987** (See also National Bureau of Standards Act; 15 USC 271)
40	759	Information systems defined
42	653	Dept. of Health and Hum Services is authorized to match welfare rolls with payroll lists to identify fraudulent welfare claims.
42	2000	**Privacy Protection Act of 1980**
42	2000	Privacy; unlawful acts

Title	Section	Description
42	2011 et seq.	**Atomic Energy Act of 1954**
44	3501	**Paperwork Reduction Act of 1980**
44	3501	OMB responsibility to provide overall direction in development and regulation of Federal information policies. Monitor compliance with Privacy Act .
45	83	Continuous lines, railroad and telegraph
47	13	Violations of laws, civil and criminal liability of carriers
47	151 et seq.	**Communications Act of 1934**
47	152	Applicability of Communications Act of 1934 to cable television
47	154	Cooperation and coordination of radio and wire communications, investigations
47	227	**Automated Telephone Consumer Protection Act of 1991**
47	305	Office of Science and Technology, war powers functions of President assigned to (See also Executive Order 12046
47	305	Telecommunications advisory committees, establishment, composition (See also Executive Order Number 12046)
47	305	Construction and operation of foreign government radio station in U.S. (See also Exec Order Number 12046)
47	305	Presentation of Executive Branch views to, functions of Secretary of Commerce
		Disclosure of information
47	305	Coordination functions of Secretary of Commerce concerning telecommunications
47	305	Telecommunications functions assigned to Secretary of Commerce
47	305	Functions assigned to OMB
47	305	Functions assigned to NSC and OSTP
47	305	Functions assigned to Department of State
47	551	Disclosure of information, protection of cable television subscriber privacy
47	605	Unauthorized use or publication of communications
47	605	Need for encryption standard in cable television
47	605	Unauthorized use or publication of communications
47	605	Foreign intelligence gathering
47	605	Blue boxes
47	605	Mobile telephone
47	605	Consent to COMSEC monitoring
47	606	Powers of President during War
47	606	Obstruction of interstate or foreign communications during War
47	609	**Federal Communications Commission Authorization Acts of 1983, 1988, 1990**
47	701-	**Communications Satellite Act of 1962**

Title	Section	Description
	744	
47	701	Communications Satellite System
47	721	Functions of FCC
47	901	**National Telecommunications and Information Administration Organization Act**
47	1001	**Communications Assistance for Law Enforcement Act of 1994** (See also amendments to 18 USC 2521 and sections of Title 47)
48	551	**Cable Communications Policy Act of 1984**
50	401	Privacy of National Security Information (See also Executive Order Number 12356)
50	401	Electronic surveillance, defined, U.S. intelligence activities (See also Executive Order Number 12333)
50	413	Congressional oversight of intelligence activities
50	1541	**War Powers Resolution Act**
50	1801 et seq.	**Foreign Intelligence Surveillance Act of 1978**
50	1801	Electronic surveillance, foreign intelligence purposes. Outside U.S.; actual or potential threat; ability of U.S. to protect against
50	1801	Electronic surveillance defined
50	1801	Consent
50	1802	Authorization of electronic surveillance without court order (See also Executive Order Number 12139)
50	1805	Approval of procedures for testing electronic surveillance equipment
50	1805	Authorization for electronic surveillance to determine existence and capability of equipment of non-authorized persons
50	1806	Disclosure of electronic surveillance methods to aggrieved party; harm to national security
50	1811	Authorization of electronic surveillance without court order; By President during time of War
50	2401 et seq.	**Export Administration Act of 1979**
50	2401 et seq.	Export of scientific and technical data
50	2510	Export of software or data controlled by DoD

This page intentionally left blank.

REGULATORY DOCUMENTS ANNOTATED BIBLIOGRAPHY

The following is an annotated bibliography of regulatory documents relevant to information warfare. Key words are also provided.

Code of Federal Regulations, Title 41, Chapter 201, *Federal Information Resources Management Regulation.*

KEY WORDS: Federal, IRM, Warner exempt

ABSTRACT: This chapter regulates the creation, maintenance, and use of Federal records and the acquisition, management and use of information processing systems. Warner exempt systems, radar, sonar, radio, and television systems are exempted.

Code of Federal Regulations, Title 47, Chapter 1, Part 63, *Rules to Provide for Notification by Common Carriers of Service Disruptions.*

KEY WORDS: FCC, NS/EP, outage reporting

ABSTRACT: This section of the Federal Communications Commission Rules and Regulations establishes outage reporting requirements. Common carriers are required to report outages potentially affecting 30,000 or more customers for 30 or more minutes. Also outages which affect special facilities, defined as 911 tandem switches, major airports, and NS/EP facilities are reported to the NCS.

Code of Federal Regulations, Title 47, Chapter II, Part 201-216, *Office of Science and Technology Policy and National Security Council.*

KEY WORDS: NS/EP, NCS, restoration priority, precedence

ABSTRACT: This chapter prescribes the conservation, allocation, and use of the Nation's telecommunications resources during crises and emergencies. It assigns responsibilities and includes NCS Directives.

Executive Office of the President, Executive Order 12333, *United States Intelligence Activities*, Washington DC, December 4, 1981.

KEY WORDS: SecDef, NSA, DoE, Attorney General, intelligence, counterintelligence, communications security

ABSTRACT: Intelligence effort to provide necessary information on which to base decisions to the President and to protect national interests from foreign security threats. Special emphasis to countering espionage directed against U.S. government, corporations, establishments or persons. Secretary of Defense named executive agent for signals intelligence and communications security activities. NSA to execute the responsibilities of the SecDef as executive agent for communications security. NSA to conduct research and development as necessary for signals intelligence and communications security. Department of Energy will support NSA as requested. Restricts collection techniques to procedures established by the agency head and approved by the Attorney General (See Foreign Intelligence Surveillance Act of 1978).

Executive Office of the President, Executive Order 12334, *President's Intelligence Oversight Board*, Washington DC, December 4, 1981.

KEY WORDS: Intelligence, oversight, national security, illegal

ABSTRACT: This order establishes the Intelligence Oversight Board and charges it with reviewing practices and procedures, investigating, and reporting to the President and the Attorney General any intelligence activities that any of the members believe to be in violation of the Constitution, laws, or presidential orders or directives. Heads of agencies, inspectors general, and general counsels will report intelligence activities they believe to be unlawful. Board members will be distinguished and trustworthy citizens outside of the government.

Executive Office of the President, Executive Order 12356, *National Security Information,* Washington DC, April 1, 1982.

KEY WORDS: National security information, classification, declassification

ABSTRACT: This EO prescribes a uniform policy for securing, classification and declassification of national security information. Revision is pending to implement changes recommended by the Joint Security Commission.

Executive Office of the President, Executive Order 12382, *President's National Security Telecommunications Advisory Committee*, Washington DC, September 13, 1982.

KEY WORDS: NSTAC, NCS

ABSTRACT: Established the NSTAC to provide the President advice and information from the perspective of industry with respect to national security telecommunications. OMNCS provides secretariat support.

Executive Office of the President, Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* Washington D.C., April 3, 1984.

KEY WORDS: NCS, NSTAC, COP, NS/EP

ABSTRACT: Established the National Communications System, an interagency group made up of 23 Federal departments and agencies. The NCS is responsible for ensuring that NS/EP telecommunications are available across a spectrum of national emergencies. NCS was to serve as a forum for government agencies and private sector. To facilitate this process, EO 12472 established the Committee of Principals for the Federal government to coordinate with the National Security Telecommunications Advisory Committee consisting of industry representatives.

Executive Office of the President, Executive Order 12881, Washington D.C.

KEY WORDS: NSTC, national goals, R&D

ABSTRACT: This EO established the National Science and Technology Council (NSTC) to establish goals for Federal science and technology investments in a number of areas including information technology. The NSTC is a cabinet -level body chaired by the President. It prepares R&D investment strategies targeting national goals that are coordinated across all Federal agencies.

Federal Communications Commission, Report and Order, *Notification by Common Carriers of Service Disruption*, FCC 92-58, Feb. 27, 1992.

KEY WORDS: PSN, outage, reporting

ABSTRACT: The purpose of this FCC Report and Order was to establish a systematic means by which to monitor, on a timely basis, major telephone service outages throughout the nation. It required local and interexchange common carriers operating transmission or switching facilities and that provide access service or interstate or international service, to promptly notify the FCC Watch Officers of any outage of 30 minutes or more with the potential to affect 50,000 or more customers. This Rule and Order followed several large PSN outages in the 1990. The reporting requirement took affect April 6, 1992 and was approved by OMB on March 23, 1992.

This page intentionally left blank.

POLICY DOCUMENTS
ANNOTATED BIBLIOGRAPHY

The following is an annotated bibliography of policy documents having applicability to information warfare/information assurance. Included are: National Security Decision Directives, National Security Directives, Presidential Decision Directives, Presidential Directives, NIST and NTIA standards and instructions, and the regulations, directives, and instructions of other organizations such as the Department of Defense. Key words are also provided. An "Index of Key Policy Documents" and an "Index of Key Implementation Standards, Guidelines, and Procedures" follow the annotated bibliographies.

Department of the Army, U.S. Army Training and Doctrine Command, *Concept for Information Operations--Final Coordinating Draft*, Jan 31, 95.

KEY WORDS: DoD, Army

ABSTRACT: Describes concept for information operations (IO), the environment, defines IO terms and relates IO to Force XXI operations.

Department of the Army, U.S. Army Training and Doctrine Command, FM 100-6, *Information Operations--Coordinating Draft*, July 22, 94.

KEY WORDS: DoD, Army

ABSTRACT: Capstone doctrinal document for incorporating information operations into "Army doctrine, individual and unit training, leader development, force design, and material acquisition initiatives."

Department of the Navy, OPNAV Instruction 3430.26, Chief of Naval Operations/N6, IW/C2W Implementing Instruction

KEY WORDS: DoD, Navy, IW/C2W, policy, joint, coordination, responsibilities, implementation

ABSTRACT: This instruction implements policy for the employment of Navy resources in support of IW/C2W and conforms to the guidance contained in previously issued directives (DoD Instruction TS3600.1, CJCS MOP 30, and OPNAVINST 3430.25). It updates previously-used terms, concepts and disciplines, and discusses the purposes of IW and C2W. The effectiveness of IW/C2W employment is stressed. Responsibilities are delineated for: CNO (N1/2/3/4/5/6/7/ 8/09N/091/095); Chief of Naval Education and Training; Naval Systems Commands; Naval Doctrine Command; Naval Security Group Command; Fleet Information Warfare Center; Naval Information Warfare Activity; Naval Criminal Investigative Service; and Fleet CINCs.

Executive Office of the President, Presidential Directive/National Security Council 24, (Declassified in 1979) Washington D.C., U.S. Government Printing Office.

KEY WORDS: NSA, DoC, NCSC, sensitive information,

ABSTRACT: Created the National Communications Security Committee which was subsequently replaced by the NTISSC and then the NSTISSC. Gave DoD authority to safeguard sensitive information that "would be useful to an adversary." Made NSA responsible for all classified information and the Department of Commerce responsible for sensitive information.

National Institute of Standards and Technology (NIST), NIST Publication List 91, *Computer Security Publications,* February 1995.

KEY WORDS: Index, COMPUSEC, NIST, publications

ABSTRACT: Index of computer security publications published by NIST/Computer Systems Laboratory. Includes special publications, reports, and Federal Information Processing Standards (FIPS) with price list and ordering information.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 186, *Digital Signature Standard (DSS),* May 1994.

KEY WORDS: DSS, DSA, digital signature

ABSTRACT: This FIPS describes a digital signature algorithm for use in applications that require both a guarantee of the identity of an originator and of the data integrity.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 28, 1994.

KEY WORDS: authentication, passwords, tokens, biometrics, COMPUSEC

ABSTRACT: This FIPS addresses alternatives to the standard use of passwords to prevent unauthorized access to computer systems. It covers authentication tokens and biometric devices.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 191, *Guideline for the Analysis of Local Area Network Security*, November 9, 1994.

KEY WORDS: COMPUSEC, LAN

ABSTRACT: This FIPS describes a security architecture for Local Area Networks, threats and vulnerabilities and security techniques.

National Institute of Standards and Technology, (NIST), NIST Internal Report Number 5424, *A Study of Federal Agency Needs for Information Technology Security*, May 1994.

KEY WORDS: DoC, DoEd, DoJ, NASA, SSA, requirements, Federal, INFOSEC

ABSTRACT: This NIST report documents the results of a study of the INFOSEC needs of the Department of Commerce, Department of Education, Department of Justice, NASA, and the Social Security Administration.

National Institute of Standards and Technology, (NIST), NIST Special Publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*, December 1993.

KEY WORDS: NIST, EC/EDI

ABSTRACT: This NIST special publication was sponsored by the Farmers Home Administration. It addresses good security practices that should be considered when developing an EC/EDI system.

National Institute of Standards and Technology (NIST), NIST Special Publication 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* U.S. Government Printing Office, Washington, 1994.

KEY WORDS: NIST, firewalls, Internet

ABSTRACT: This NIST special publication provides an overview of the Internet, Internet security problems and firewalls. It is written in an elementary, non-technical style and refers the reader to sources of additional information.

National Security Agency (NSA), National Telecommunications and Information Systems Security Directive No. 600, *Communications Security Monitoring*, April 10, 1990.

KEY WORDS: COMSEC monitoring, government telecommunications, privacy

ABSTRACT: States that government telecommunications systems are subject to monitoring by authorized government agencies. Applies to official telecommunications of Federal government employees, contractors, and other entities when transmitted over government owned or leased telecommunications systems. Government telecommunications and telecommunications systems defined.

National Security Decision Directive (NSDD) 145, 1984.

KEY WORDS: NSTISSC, EOP, unclassified information

ABSTRACT: Created (reestablished) the interagency group National Security Telecommunications and Information Systems Security Committee (NSTISSC) and required protection of sensitive unclassified information as well as classified information. NSDD 145 was rescinded by NSD 42.

National Security Decision Directive (NSDD) 298, 1988.

KEY WORDS: Policy, EOP, directive, OPSEC, NSA, IOSS

ABSTRACT: Mandated implementation of a formal OPSEC program by each executive department and agency with national security responsibilities. Designated Director, NSA, as executive agent for OPSEC programs and tasked him to establish and maintain an Interagency OPSEC Support Staff (IOSS).

National Security Directive 42, July 5, 1990.

KEY WORDS: SecDef, NSA, NSTISSC, COP, CIA, COMSEC monitoring, National Manager, vulnerability, Federal government

UNCLASSIFIED ABSTRACT: NSD 42 revised NSDD 145 with the objective of improving U.S. government capabilities for securing national security systems against technical exploitation and implementing countermeasures. SecDef is executive agent and Director, NSA designated as the National Manager and charged with examining national security systems and evaluating their vulnerability. Defines telecommunications, information systems, and national security systems. Reestablishes the national Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISSC is tasked to develop policies, procedures, guidelines, instructions, standards, objectives, and priorities and systems security guidance, approve the release of cryptographic material to foreign governments with CIA concurrence, establish a national system for promulgating operating policies, instructions, directives, guidance, etc. and to interact with the National Communications Systems Committee of

Principals established by Executive Order 12472. NSA provides a supporting secretariat.

Office of Management and Budget (OMB), Circular A-123, *Internal Control Systems*, Washington DC, U.S. Government Printing Office, August 16, 1983.

KEY WORDS: OMB, fraud, waste, abuse, internal controls, accountability

ABSTRACT: Requires executive agencies to establish management plans to eliminate fraud, waste , and abuse.

Office of Management and Budget (OMB), Circular A-130, *Management of Federal Information Resources* Washington DC, U.S. Government Printing Office, December 1985.

KEY WORDS: OMB, sensitive information, security, security programs

ABSTRACT: Made the head of each agency responsible for information technology security. Required all Federal information systems to provide security commensurate with the sensitivity of the data in the system. Agencies will establish security programs to safeguard sensitive information.

Office of Management and Budget (OMB), Circular A-130 (Revised), *Policy on Open Systems.*

KEY WORDS: OMB, Federal government, policy, security

ABSTRACT: The revised A-130, a capstone federal information systems policy document, provides uniform government-wide information resources management policies. A-130 is being revised in phases. Transmittal Memorandums Number 1 (June 25, 1993) and 2 (July 25, 1994) have been issued. Appendix III, Security has been published for comment. The Appendix III revision aligns Federal government security responsibilities with the Computer Security Act. It requires assignment of security responsibilities, requires security plans for all general support computer systems and stresses management controls and risk management.

Office of Management and Budget (OMB), National Information Infrastructure Security Issues Forum, *NII Security: The Federal Role,* Washington DC, June 14, 1995.

KEY WORDS: OMB, NII, IITF, security, federal role.

ABSTRACT: The Security Issues Forum and the U.S. Advisory Council (NII) held seven public meetings with government officials and representatives of the public and private sector. Users and service providers were represented at these

meetings. The feedback received at these meetings has been incorporated into this report. The report, issued for comment, "summarizes the Forum's findings concerning security needs in the National Information Infrastructure (NII); presents an analysis of the institutional, legal, and technical issues surrounding security in the NII; and proposes Federal actions to address these issues." The report defines security in the NII to include integrity, availability, and confidentiality of information and reliability of systems. Findings for action include: (1) adoption of the proposed NII Security Tenets, (2) adoption for the NII of the Organization for Economic Cooperation and Development (OECD) Security Principles, and (3) implementation of the Federal role as recommended in the report. Federal roles include stimulating security issues dialogue and awareness, making Federal security products and techniques available for use on the NII, and promoting private sector development of security products and services. Additionally, "In its role as protector of the public interest, the government will: (1) assure adequate emergency response capability on the NII; (2) adapt current oversight processes to meet the challenges of the NII; (3) review criminal law; and (4) promote international cooperation.

Office of the Secretary of Defense, DoD Directive 8000.1, *Defense Information Management Program*, October 27, 1992.

KEY WORDS: DoD, policy,

ABSTRACT: Director, DISA will "in consultation with the Directors of the DIA and NSA, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

INDEX OF KEY POLICY DOCUMENTS

Policy Documents
Air Force Regulation 205-16 (superseded by AFSSI 5100)
Air Force Regulation 56-1 (superseded by AFSSI 4100)
Air Force Regulation 57-1, Operational Needs, Requirements, and Concepts
Air Force Regulation 400-26, Logistics Support for Ground Communications-Electronic Systems and Equipment
Air Force Regulation 700-1, Managing Air Force Communications-Computer Systems
Air Force Regulation 700-2, Communications-Computer Systems Planning and Architectures
Air Force Regulation 700-3, Information Systems Requirements Processing
Air Force Regulation 700-4, Volume I: Information Systems Program Management, Volume II: Information System Acquisition and Major Automated Information Systems Review Requirements
Air Force Regulation 800-1, Air Force Acquisition System
Air Force Instruction 31-40, Information Security Program Management
Army TRADOC, PAM 525-XX, Concept for Information Operations, Final Coordinating Draft
Army TRADOC, FM 100-6, Information Operations, Coordinating Draft
Army Regulation 380-19, Information Systems Security
Army Regulation 380-5
Army Regulation 380-40, Policy for Safeguarding and Controlling COMSEC Material
Army Regulation 525-20
Army Regulation 25-1, The Army Information Resources Management Program
Army Regulation 25-3, Army Life Cycle Management of Information Systems
Army Regulation 70-1, Army Acquisition Policy
CJCS, National Military Strategy Document, App. C, C4 Systems
CJCS MOP 3, Command, Control, & Communications Countermeasures
CJCS MOP 6, Electronic Warfare
CJCS MOP 10, Near Real Time Analysis of EMI and Jamming of U.S. Space Systems
CJCS MOP 24, Tactical Employment of Directed Energy Combat Systems
CJCS MOP 30, Command and Control Warfare
CJCS MOP 43, Military Telecommunications Agreements and Arrangements between the U.S. and Regional Defense Organizations or Friendly Foreign Nations
CJCS MOP 52, Policy and Responsibilities for the Denial of Environmental Information to an Enemy
CJCS MOP ??, Information Resource Management
CJCS Instruction 6211.02, Defense Information System Network and Connected Systems
CJCS Instruction 6212.01, Compatibility, Interoperability, and Integration of C3I Systems
CJCS Instruction 6510.1, Joint and Combined Communications Security
CJCS, Joint Pub 1, Joint Warfare of the U.S. Armed Forces
CJCS, Joint Pub 1-02, Dictionary of Military Terms

CJCS, Joint Pub 3-13, Doctrine for Command and Control Warfare (C2W)
CJCS, Joint Pub 3-53, Doctrine for Joint Psychological Operations
CJCS, Joint Pub 3-54, Joint Doctrine for Operations Security
CJCS, Joint Pub 3-58, Joint Doctrine for Military Deception
COMSEC Program Publications, Various DoD, NSA
Federal Information Resources Manual (IRM)
Marine Corps Order 3430.5A, Policy for Command & Control Warfare (C2W)
Marine Corps Publication 5510.14, Marine Corps Automatic Data Processing Security Manual
NCSC Policy 1, National Policy for Safeguarding and Control of Communications Security Material
NCSC Policy 2, National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernment Sources
NCSC Policy 3, TEMPEST Glossary
NCSC Policy 5, National Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments
NCSC Policy 6, National Policy Governing the Disclosure or Release of Communications Security Information to Foreign Governments and International Organizations
NCSC Policy 8, National Policy on Secure Voice Communications
NCSC Policy 11, Policy for National Security Information Carried by Any Transmission System By Government or Contractors
Naval Doctrine Publication 1, Naval Warfare, Volume 6, Command and Control
Navy, OPNAVINST 3430.25, Information Warfare and Command and Control Warfare
Navy, OPNAVINST 3430.26, Implementing Instruction fro Information Warfare (IW)/Command and Control Warfare (C2W)
Navy, OPNAVINST 5239.1A, Department of the Navy ADP Security Manual
Navy, OPNAVINST 5290.1A, Naval Imaging Program Policy and Responsibility
Navy, OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation
Navy, OPNAVINST C5510.93E, Navy Implementation of National Policy on Control of Compromising Emanations
Navy, OPNAVINST 5530.14B, Department of the Navy Physical Security and Loss Prevention Manual
Navy, SECNAVINST 5000.2A, Implementation of Defense Acquisition Management Policy-Procedures Documentation and Report
Navy, SECNAVINST 5200.32A, Acquisition Management Policies and Procedures for Computer Resources
Navy, SECNAVINST 5231.1C, Life Cycle Management Policy and Approval Requirements for Information System Projects
Navy, SECNAVINST 5233.1B, Department of the Navy Automated Data Systems Documentation Standards
Navy, SECNAVINST 5238.1C, Computer Resources Management
Navy, SECNAVINST 5239.2, Department of the Navy AIS Security Program

Navy, SECNAVINST 5400.15, Department of the Navy Research, Development, and Acquisition Responsibilities
Navy, SECNAVINST 5510.30, Department of the Navy Personnel Security Program
NSA, National Policy for the Security of National Telecommunications and Information Systems
NSD 42, (Revised NSDD 145)
NSDD 97, National Security Telecommunications Policy
NSDD 145, Protection of Both Classified and Sensitive Information; Interagency Structure for Computer Security
NSDD 189, Reporting of Unclassified Research
NSDD 298
OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Standards
OMB Circular A-123, Internal Control Systems
OMB Circular A-127, Financial Management Systems
OMB Circular A-130, Management of Federal Information Resources
OSD, Defense Management Review Decision (DMRD) 918
OSD, DoD Directive 3222.4, Electronic Warfare and Command and Control Warfare (C2W) Countermeasures
OSD, DoD Directive TS 3600.1, Information Warfare
OSD, DoD Directive 4640.6, Communication Security Telephone Monitoring and Recording
OSD, DoD Directive 5000.1, Defense Acquisition
OSD, DoD Directive 5100.1, Functions of the DoD and Its Major Components
OSD, DoD Directive 5100.30, World-wide Military Command and Control System (WWMCCS)
OSD, DoD Directive 5105.19, Defense Information Systems Agency
OSD, DoD Directive 5200.1, DoD Information Security Program
OSD, DoD Directive C-5200.2, Department of Defense Personnel Security Program
OSD, DoD Directive C-5200.5, Communications Security (COMSEC)
OSD, DoD Directive C-5200.8, Security of DoD Installations and Resources
OSD, DoD Directive S-5200.16, Objectives and Minimum Standards for Communications Security Measures used in Nuclear Command, Control, and Communications
OSD, DoD Directive C-5200.19, Control of Compromising Emanations
OSD, DoD Directive 5200.28, Security Requirements for Automated Information Systems
OSD, DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria
OSD, DoD Directive 5205.2, DoD Operations Security Program
OSD, DoD Directive O-5205.7, Special Access Program Policy
OSD, DoD Directive C-5215.1
OSD, DoD Directive 5220.22, DoD Industrial Security Program
OSD, DoD Directive 5240.11, Damage Assessments
OSD, DoD Directive 7750.5, Management and Control of Information Requirements
OSD, DoD Directive 8000.1, Defense Information Management Program
OSD, DoD Directive 8320.1, DoD Data Administration

OSD, DoD Regulation 5200.1-R, Information Security Program Regulation
OSD, DoD Manual 5000.2-M, Defense Acquisition Management Documentation and Reports
OSD, DoD Manual 5200.28-M, Automated Information System Security Manual
OSD, DoD Manual 8020.1-M Management Guidance on Functional Process Improvement
OSD, DoD Instruction 5000.2, Defense Acquisition Management Policies and Procedures
OSD, DoD Instruction 5240.11, Damage Assessments
OSD, DoD Instructions, 8000 Series Information Management
8000-8099 Defense Information Management
8100-8199 Information Systems
8200-8299 Information Services
8300-8399 Data Management
8400-8499 Information Technology
8900-8999 Information Collection and Dissemination
OSD, DoD Instruction 8000.2, Defense Information Management Policies and Procedures
OSD, DoD Instruction 8020.1, Functional Process Improvement Program
Presidential Directive/National Security Council 24
Presidential Directive 53, National Security Telecommunications Policy

INDEX OF KEY IMPLEMENTATION STANDARDS, GUIDELINES, AND PROCEDURES

Implementation Standards, Guidelines, and Procedures
COMSEC Program Publications
Summary of the Commercial COMSEC Endorsement Program (CCEP)
Handling and Control of Controlled Cryptographic Items During Development and Manufacture/Assembly
Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M)
COMSEC Supplement to DoD Industrial Security Manual (DoD 5220.22-S)
Industrial COMSEC Material Control Manual
U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual
DCID 1/16 Handling of Intelligence Information
DIA, Security Requirements for System High and Compartmented Mode Workstations
DIA, Compartmented Mode Workstation Evaluation Criteria
DIA, Compartmented Mode Workstation Standard user Interface Style Guide
DIA Manual 50-3
DIA Manual 50-4
DIA Manual 50-5
DIA Manual 50-6
DIA Manual 50-8
DIA Manual 50-24
DIA Manual 50-28
National Communications Security (COMSEC) Instructions (NACSI), 12 Titles
National Communications Security (COMSEC) Information Memoranda (NACSIM), 3 Titles
National Communications Security (COMSEC) Emanations Memoranda (NACSEM), 9 Titles
NIST, FIPSPUB 31 Guidelines for ADP Physical Security and Risk Management
NIST, FIPSPUB 39, Glossary for Computer Systems Security
NIST, FIPSPUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974
NIST, FIPSPUB 46-1, Data Encryption Standard
NIST, FIPSPUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification
NIST, FIPSPUB 65, Guideline for Automated Data Processing Risk Analysis
NIST, FIPSPUB 73, Guidelines for Security of Computer Applications
NIST, FIPSPUB 74, Guidelines for Implementing and using the NBS Data Encryption Standard
NIST, FIPSPUB 81, DES Modes of Operations
NIST, FIPSPUB 83, Guideline on User Authentication Techniques for Computer Network Access Control
NIST, FIPSPUB 87, Guidelines for ADP Contingency Planning
NIST, FIPSPUB 88, Guideline on Integrity Assurance and Control in Database Administration
NIST, FIPSPUB 94, Guideline on Electrical Power for ADP Installations

NIST, FIPSPUB 102, Guidelines for Computer Security Certification and Accreditation
NIST, FIPSPUB 112, Standard on Password Usage
NIST, FIPSPUB 113, Standard on Computer Data Authentication
NIST, FIPSPUB 139, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications
NIST, FIPSPUB 140, General Security Requirements for Equipment Using the Data Encryption Standard
NIST, FIPSPUB 141, Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment
NIST, FIPSPUB 179, Government Network Management Profile
NIST, FIPSPUB 185, Escrowed Encryption Standard
NIST, FIPSPUB 186, Digital Signature Standard
NIST, FIPSPUB 188, Standard Security Label for Information Transfer
NIST FIPSPUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives
NIST FIPSPUB 191, Guideline for the Analysis of Local Area Network Security
NIST Internal Report 5424, A Study of Federal Agency Needs for Information Technology Security
NIST Special Publications, Various Titles
NSA, National Computer Security Center, Rainbow Series, Various Titles
NTISS/NSTISS Directive 500, Information Systems Security (INFOSEC) Education, Training, and Awareness
NTISS/NSTISS Directive 501, National Training Program for Information Systems Security (INFOSEC) Professionals
NTISS/NSTISS Directive 502, National Security Telecommunications and Automated Information Systems Security
NTISS/NSTISS Directive 503, Incident Response and Vulnerability Reporting for National Security Systems
NTISS/NSTISS Directive 600, Communications Security Monitoring
NTISS/NSTISS Directive 900, Governing Procedures of the National Security Telecommunications and Information System Security Committee (NSTISSC)
NTISS/NSTISS Directive 901, National Telecommunications and Information Systems Security Issuance System
NTISS/NSTISS Instructions 3000-3020 (21 Titles), Operational Security Doctrine for Various Cryptographic-Based Systems
NTISS/NSTISS Instruction 4000, Communications Security Equipment Maintenance and Maintenance Training
NTISS/NSTISS Instruction 4001, Controlled Cryptographic Items (CCI)
NTISS/NSTISS Instruction 4002, Classification Guide for COMSEC Information
NTISS/NSTISS Instruction 4003, Reporting and Evaluating COMSEC Incidents
NTISS/NSTISS Instruction 4004, Routine Destruction and Emergency Protection of COMSEC Material
NTISS/NSTISS Instruction 4005, Control of Top Secret Keying Material

NTISS/NSTISS Instruction 4006, Controlling Authorities for COMSEC Material
NTISS/NSTISS Instruction 4007, COMSEC Utility Program
NTISS/NSTISS Instruction 4008, Program for the Management and Use of National Reserve Information Systems Security (INFOSEC) Material
NTISS/NSTISS Instruction 4009, National Information Systems Security (INFOSEC) Glossary
NTISS/NSTISS Instruction 4010, Keying Material Management
NTISS/NSTISS Instruction 4011, National Training Standard for INFOSEC Professionals
NTISS/NSTISS Instruction 7000, TEMPEST Countermeasures for Facilities
NTISS/NSTISS Instruction 7001, NONSTOP Countermeasures
NTISS/NSTISS Policy 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems
NTISS/NSTISS Policy 3, National Policy for Granting Access to U.S. Classified Cryptographic Information
NTISS/NSTISS Policy 4, National Policy on Electronic Keying
NTISS/NSTISS Policy 5, National Policy for Incident Response and Vulnerability Reporting for National Security Systems
NTISS/NSTISS Policy 8, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
NTISS/NSTISS Policy 100, National Policy on Application of Communications Security to Command Destruct Systems
NTISS/NSTISS Policy 200, Controlled Access Protection (C2 by '92)
NTISS/NSTISS Policy 300, National Policy on Control of Compromising Emanations
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 3 Titles, COMSEC Advisories
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 4 Titles, COMPUSEC Advisories
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 6 Titles, TEMPEST Advisories
OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
OMB Bulletin 91-10, Information Resources Management (IRM) Plans Bulletin
OMB Bulletin 92-05, Information Resources Management (IRM) Plans Bulletin
OMB, OMB Bulletin 88-16, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information
Other Security-Relevant Government Publications
OTA, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information
OTA, Federal Government Information Technology: Management, Security, and Congressional Oversight
OTA, Federal Government Information Technology: Electronic Surveillance and Civil Liberties
OTA, Federal Government Information Technology: Electronic Record Systems and Individual Privacy
TEMPEST Program Publications
NSA Objective Standards for Product Assurance
Endorsed TEMPEST Products Program

Endorsed TEMPEST Test Services Program
Endorsed TEMPEST Test Instrumentation Program
PPL Product Transition Guidelines and Procedures
PPL Accreditation Standard Operating Procedures and Requirements
ITP Quality Assurance Procedures
ITP Standard Operating Procedures

PERIODICAL ARTICLES
ANNOTATED BIBLIOGRAPHY

"A-130 Embraces State, Local Govts.; OMB's Revamped IT Circular Expands Scope of Information Dissemination," *Government Computer News*, Vol. 13, No. 18, Page 83, August 15, 1994.

KEY WORDS: OMB, Circular A-130, Regulatory

ABSTRACT: "The Office of Management and Budget's (OMB) revamped Circular A-130 states that agency plans for information dissemination should integrate the needs of state and local governments, and that online databases stored on CD-ROM should be managed as information products, not services....The document also suggests that agencies develop performance measures to ensure maximum ROI on their IT investments....First issued in 1985, A-130 is the government's basic information technology policy document....Many of the changes are consistent with previous drafts and follow the National Performance Review's strategy for using IT to improve public services, increase public access to Federal information and better gauge program performance....The administration has been retooling the circular in stages. OMB officials still are working on proposed modifications to detailed portions of A-130 covering information security and IT oversight."

Anthes, Gary H.; "Guarding the Internet," *Computerworld*, Vol. 28, No. 35, Page 55, August 29, 1994.

KEY WORDS: Internet, privacy, integrity, authentication, firewall, policy, filters, Mosaic, Arpanet, encryption, NISPPAC, NISP, ISOO, transportation, Air Force, Senate Armed Serviced Committee

ABSTRACT: " 'The Internet provides no security, no assumption of privacy, no expectation of integrity and no assumption of authentication,' said Michael P. Ressler, a member of Bellcore's Secure Communications & Services Group....'Benefits of an Internet connection outweigh its risks.
E-mail alone would lead you to connect,' he said....Connecting to the Internet is inevitable for most companies, according to Ressler. You might as well face it: 'Your employees will connect to the Internet,' he said. You cannot enforce a prohibition against modems. Ressler said it is easier to establish usage policies before employees connect to the Internet than it is afterward....'The sooner you provide controlled access, the less likely you are to have uncontrolled access,' he said....Kenneth J. Cutler, a vice president at the Information Security Institute said 'Internet Protocol *packet filters* in firewalls may be too restrictive, inconveniencing users and slowing performance.'...Three weeks ago, tiny NetMarket Co. in Nashua, N.H., became the first company to offer an encrypted

credit-card transaction service over the Internet. Using a public-key encryption technology called Pretty Good Privacy."

Arnst, Catherine; Burrows, Peter and Kelly, Kevin; "Phone Frenzy," *BusinessWeek*, Page 92, February 20, 1995, McGraw-Hill.

KEYWORDS: Information Industry Association, NII, government databases

ABSTRACT: "Open markets and technologies such as fiber optics and wireless transmission that create huge amounts of low-cost calling capacity mean that just about anyone who wants to become a phone company can....Mergers, alliances, new entrants, and new services are already changing the telecom landscape. Phone companies want into cable. Cable operators will sell phone service. Long-distance companies will take on local carriers -- and vice versa. And everyone will seek 'content' -- from electronic yellow pages to movies -- to lure traffic onto the emerging Information Superhighway....Certainly it will be confusing at first, but a decade of deregulation in long distance has conditioned Americans for what's ahead. After all, until 1984 nobody had ever thought about choosing a long-distance company....The driving force behind today's phone frenzy is technology. Most striking is fiber-optic cable. Conventional twisted-pair copper phone wires carry only a few conversations at a time. But a single glass strand can carry at least 32,000 conversations at once....All this capacity means that a network can handle a virtually unlimited amount of traffic and add new services with almost no new capital investment....there's still one obstacle to remove: a regulatory framework based on the notion of phone service as a 'natural' monopoly....'The idea of the natural monopoly has lost all credibility around the world,' says Ken Zita, a partner with the consulting firm Network Dynamics Associates Inc. in New York....There is virtual agreement in the telecommunications industry, on Capitol Hill, and in the statehouses that deregulating local service will be a boon to the nation. For proof, look at what happened in long distance. Since 1984, carriers have tripped over each other to add new services, and their market-share battles have sliced rates more than 60%. Competition could do the same in local calling, says Senator Larry Pressler (R-S.D.), chairman of the Senate commerce Committee: 'Progress is being stymied by a morass of regulatory barriers that balkanize the telecommunications industry.'...An econometric study done by the consultancy WEFA Group Inc. -- sponsored by the Baby Bells, mind you -- estimates that competition in local calling will spark so much demand for new services that there will be a net gain of 3.6 million jobs by 2003. That's in addition to 1 million phone workers today. When will it all happen? Much depends on Congress. Pressler now leads the effort to replace vintage 1934 regulations....Pressler has outlined a bill allowing competitors into local calling immediately but keeping the regional Bell operating companies (RBOCS) out of long distance and cable for one to three years. The Bells want simultaneous entry, while long-distance and cable companies want local carriers shackled until there's measurable local competition....Nynex Corp., the regional Bell, is cooperating with New York regulators -- because deregulation will let the $13.3 billion phone giant leap into all sorts of new businesses such as long distance and cable TV....Nynex took another big step into the competitive era on Jan. 25, when it announced plans to treat MFS Communications Co., a competitive access provider that links business customers to long-distance carriers, as a co-equal common carrier. It's the first such pact between an RBOC and a rival....They could even get service from the New York State Thruway Authority. It's gauging the feasibility of laying fiber-optic cable along its rights-of-way and offering phone service....Morgan Stanley & Co. calculates that phone services should add 8% to 10% to a cable system's value. Also, coaxial wiring can handle broadband speeds right away, so it will be cheaper for companies to add voice than for phone companies to add video....Some of the nation's top cable-TV operators--Tele-Communications, Cox Enterprises, and Comcast -- have formed an alliance with Sprint to build and operate a nationwide wireless phone network....The confusing blur between cable and phone operators is intentional: Executives in both industries say their futures may depend on it. 'We're going to be an integrated communications company with telephony, video -- which is our core -- and new products: interactive audio and video products.'...U.S. West Inc. is furiously repositioning itself for video, paying $2.5 billion for 25.51% of Time Warner and launching video-on-demand trials. U.S. West, Bell Atlantic, Bell South, Ameritech, and Nynex have all won Federal court rulings allowing them to provide video over phone lines, also known as video dial tone. On Jan. 29, a Federal court gave the same right to most of the nation's small phone companies....Anyone who can make a deal with MCI Communications Corp. or AT&T to buy capacity at bulk rates can become a reseller....Deregulation will change that. The Bells expect to get into long distance, but long-distance carriers also expect to get into local service -- in part to slash access fees. Each of the big three of long distance is preparing direct local connections....All the local phone companies are furiously trying to look less like prey. They're spending billions to create stronger brand names and build broadband networks. Pacific Telesis plans to spend $16 billion over seven years; Bell Atlantic has budgeted $11 billion; U.S. West $10 billion; Southern New England Telecommunications $4.4 billion....'By Catherine Arnst in New York, with Kevin Kelly in Chicago, Peter Burrows in Dallas, and bureau reports.' "

Arnst, Catherine and Michael Oneal, "The New Era Begins in Rochester," *BusinessWeek*, Page 97, February 20, 1995, A McGraw-Hill Publication.

KEYWORDS: local service, competition

ABSTRACT: "Rochester, N.Y. On Jan. 1, it became the first U.S. city in 75 years to allow residents a choice of local carriers. Rochester Telephone Corp. lets any and all comers connect to its network and its customers. The reward: an end to Rochester Tel's state-mandated profit limits and the right for it to offer long-distance and video services. The agreement makes this Great Lakes community of 750,000 a test bed for the telecommunications battle to come....Rochester Tel is not a Bell. Founded in 1899, it managed to avoid joining the vast Bell system and so escaped the many restrictions placed on the regional operating companies when AT&T was broken up....As a result, Rochester Tel -- now reorganized as the local service arm of the Frontier Corp. holding company -- has always been able to offer long distance outside its service region....Rochester Tel proposed ending its monopoly in return for an end to profit caps and freedom to compete. It agreed to cut rates 11% and freeze basic residential fees for seven years. Customers can keep their phone numbers if they switch carriers, and competitors must be allowed to connect seamlessly to the local network. Time Warner is determined to make Rochester more than an experiment. It has some 200,000 cable customers there and is upgrading its network for telephony. 'We'll have dial tone by the third quarter sometime.'...'By Catherine Arnst in Rochester, with Michael Oneal in New York.' "

"AT&T And VLSI In Security Pact," *Information Week,* Issue 514, February 13, 1995, page 26.

KEYWORDS: Encryption, Clipper, AT&T

ABSTRACT: AT&T and semiconductor manufacturer VLSI have teamed to produce and distribute cryptographic chips and can be employed in numerous products including PCs, cellular phones and Cable TV. The first product will be available in late 1995 and used in the pay-per-view and video-on-demand markets. This alternative to software encryption will compete with the NSA-approved Clipper chip.

"Background - Report on Commission's Plans Re - Information Society," *Spicers Centre for Europe, European Report C/c 12/85 (SPICEU,ER),* October 14, 1994.

KEY WORDS: Policy, European Union

ABSTRACT: "Report on a series of proposals and documents that the Commission is to release on the information society....These include: an Action Plan stressing the need to agree on dates for exposing infrastructure to competition; a communication on the general approach to be taken; a Green Paper on the same subject; a report on leased lines; proposals on guaranteeing the inter-connection and inter-working of networks; a communication on the audiovisual sector; a Green Paper on the protection of intellectual property in the information society; a draft Directive on home copying of audio and video tapes; a Green Paper on the legal protection of coded broadcasts; a proposal on coding in business; a communication on information security matters; an 'overall conceptual framework'; and a draft Directive on liberalizing satellite telecommunications."

"Bankers, Other Groups Warn of NII Sabotage, Theft, Fraud," *Telecom Data Report*, Vol. 3, No. August 1, 1994.

KEY WORDS: banking, NII, Association, NII Security Issues Forum, DES, encryption policy, Clipper Chip, Digital Signature Standard

ABSTRACT: "The nation's banking community told the administration July 15 it has serious concerns about the purported commercial advantages of a National Information Infrastructure (NII) made up of interconnected digital networks....The American Bankers Association (ABA), in testimony to the NII Security Issues Forum....The ABA urged the government to extend current efforts to share advanced security technology with the banking industry. The group also warned that the government's decision to abandon the Digital Encryption Standard (DES) technology could create havoc as the industry rushes to find a substitute. The banker's group urged telephone companies to beef up network security and reliability....The Department of Commerce has certified DES as an encryption standard for the next five years. Among its concerns, the ABA requested more time to find a replacement for DES, and said the two-party key escrow system 'must provide for at least one of the key parts to be held only by a private-sector entity, such as a clearinghouse or a *big six* accounting firm.'...Thirty-one organizations representing commerce and banking, manufacturing, health services, electronic publishing, education and government services presented their concerns....Nanette DiTosto of the U.S. Council on International Business, a New York-based group representing multinational corporations, law firms and business organizations, said the choice of security technology should be left to the end user, leaving network providers to concentrate on making public network services more available....Business needs internationally accepted means for ensuring the privacy, integrity, confidentiality, authenticity and nonrepudiation of communications and information transfer....Fax papers to (202) 622-2057 or message via the internet to nii.security@treas.sprint.com. For more information call Marty Ferris at (202) 622-1110 or Virginia Huth at (202) 395-3785. Copyright 1994 BRP Publications."

Barr, Stephen ; "Downsizing: Whose Jobs Will Be Cut?," *The Washington Post*, Page 1, April 3, 1995.

KEYWORDS: Downsizing, disgruntled employees

ABSTRACT: "The wave of 'downsizing' that is rolling toward the Federal government is beginning to splash nearly every Cabinet department. ..... The politicians are talking about cutting whole Cabinet agencies -- making changes that could fundamentally reshape the Federal work force of 2.1 million people and alter the character of the Washington regional economy. ..... Federal workers understandably are worried about what lies ahead, for themselves and their families. ..... The Clinton administration and Congress have agreed to cut 272,900 Federal workers by 1999. The administration expects to have trimmed about half that total by the end of September, leaving 135,400 jobs to be cut over the next four years. The main of these job cuts has been eased, thus far, by 'buyouts.' But 1996 and 1997 may prove to be tougher times. ..... The most dramatic job cuts have come in the defense sector, because of the post-Cold War reduction in the size of the military. The drop in Defense Department civil service employees over the past few years has been staggering -- from 1.1 million in fiscal 1989 to a projected 799,000 by fiscal 1997. ..... Only about 5,000 employees received involuntary separations last year. ..... The pace quickened last week, when Clinton and Vice President Gore announced $13 million in cuts at four more agencies -- the Interior Department, the National Aeronautics and Space Administration, the Small Business Administration and the Federal Emergency Management Agency. ..... The Kasich aide suggested that the Departments of Commerce and Energy may be the first to sink ..... American University professor James A. Thurber said. 'There is an extraordinary, hostile environment for public service right now,' ..... The Park Service undertook a restructuring program that prompted 'a fair amount of anxiety and distress' among employees, Gorrell said, even though managers tried to keep the staff up to date on plans to reduce headquarters staffing and shift more employees to national parks. 'There was so much doggone uncertainty that the anxiety took on a life of its own,' he aid. 'No matter how much you told people, they didn't know what was going to happen to them personally, to their organization or to their budgets. That's tough to live with on a daily basis."

Bartsch, Adam; "Feds Plead Fifth on Security," *Computer Digest*, Vol. 10, No. 1, Page 15, January, 1995, Calmers Publishing Company.

KEY WORDS: Federal government, DoE, GAO, DoS, IRS, firewalls

ABSTRACT: "Computer security is generally responsive, very rarely is it proactive, Mark Bentley said....And penetrations abound, particularly since the Internet became such an inviting gateway for computer users to reach the outside world....Several Federal agencies indicated that, at a minimum, they have installed, or intend to install, a firewall to restrict their exposure to the outside world....The Department of Energy hasn't opened itself up to the outsiders yet, according to Brent Frampton, computer security specialist for the agency's Energy information Administration....General Accounting Office....The Department of State does its own testing, assessments and evaluations of security methods in its computer security laboratory....Jules Romagnoli, chief of the Assessment and Certification Division, bureau of Diplomatic Security at the State Department....The Internal Revenue Service (IRS) is reviewing many security technologies as it gears up to install systems that will protect many separate levels of sensitive information. We are absolutely going to be using encryption, said Jim Robinette, a security specialist for the IRS....For revenue agents that travel around the world and carry a laptop with them, there will have to be an encryption capability for the data that is in that machine. We're not going to have a laptop with data in the clear. Additionally, the IRS will employ augmented identification and authentication methods, most likely in the form of a smartcard or thumbprint. Another capability under review is a small tape drive with a tiny cartridge that holds a gigabyte of data and can be password encrypted....Infrared camera sitting on the bottom of your screen and if someone walks behind you close enough to where they could read the information on the screen, it blanks the screen....Employees perform basic daily security measures....State Department security administrators are looking to the assistant secretaries to take responsibility for security of systems under their direction."

Bass, Brad, "Federal Encryption Policy Shifts Direction," *Federal Computer Week,* Page 28, February 20, 1995.

KEYWORDS: Clipper, RSA, DSS, DES

ABSTRACT: "The Clinton administration appears to be backing away from its controversial Clipper/Capstone voice and data encryption plan, instead favoring a public-key approach supported by industry. ..... In February the White House asked a panel of experts from NIST, the National Security Agency and the FBI to formally evaluate an alternate key escrow system developed by Trusted Information Systems Inc. (TIS), ... Under the TIS proposal, users would register with and receive public keys from data-recovery centers established at their agencies or private organizations. This proposal would replace Clipper and Capstone but not DSS. ..... Bruce Falls, the Federal region sales manager at Network Systems Corp., Minneapolis, said he sees a burgeoning market for encryption in the Federal government. ..... 'Encryption is not a requirement for only intelligence in the government anymore. It's now in commercial enterprise, civilian agencies or anybody connected to the Internet.' ..... Hank Philcox, chief information officer at the IRS, said the agency uses link encryption on its wide-area connections but is testing products that could extend that capability to modems and public lines. ..... He said agency personnel are considering an acquisition of Fortezza PCMCIA cards like those to be included in the Defense Message System. Fortezza cards incorporate Capstone key escrow encryption and DSS to secure electronic-mail messages. ..... DSS has provoked a barrage of criticism because few commercial products conform to the standard. To make matters worse, many commercial organizations have embraced a competing digital signature algorithm created by RSA Data Security Inc., ... Unlike DSS, which provides only digital signatures, the RSA algorithm signs and encrypts messages, essentially doing the work of Capstone and DSS combined. Analyst John Pescatore of IDC Government, Falls Church, Va. said RSA has come to dominate the encryption market, ... 'The government is not the big one doing EDI; the auto industry and the banking industry are. The government is small potatoes.' ..... McNulty said Fortezza cards will cost $100 to $125 per user and an additional $50 to $75 for a PCMCIA slot if necessary."

Status: Clinton administration officials appear to backing off from their mandated Clipper and Capstone voice and data encryption standards.

Issues: How will this affect Federal users of encryption products, particularly civilian agencies that need encryption for electronic commerce applications? Will the lack of support for Clipper and Capstone move more users to RSA and undermine the Digital Signature Standard too?

Outlook: Unclear. A White House panel considering commercially available alternatives to Clipper and Capstone will finish its report within the next three months.

Federal Encryption Standards:

Clipper:

Definition: A chip with embedded voice-encryption capability that has a backdoor for law enforcement purposes.

Vendor: Mykotronx

Rival technology: Triple DES

Rival vendor: AT&T and VLSI

Capstone:

Definition: A chip with embedded data-encryption capabilities that has a backdoor for law enforcement purposes.

Vendor: Mykotronx

Rival technology: Triple DES

Rival vendor: AT&T and VLSI

Digital Signature Standard:

Definition: An algorithm that provides digital signatures to ensure authenticity.

Vendors: AT&T, Fischer International

Rival technology: RC5

Rival vendor: RSA Data Security"

Bass, Brad, "NIST group attacks plan on security issues," *Federal Computer Week*, Page 4, December 19, 1994.

KEYWORDS: Federal, e-mail, NIST, GSA, OMB

ABSTRACT: "A plan for installing governmentwide electronic mail came under attack last week from a National Institute of Standards and Technology group for providing inadequate security and privacy safeguards. ..... Board chairman Willis Ware, a corporate research staff member at the Rand Corp., said the board members thought GSA's E-Mail Program Management Office has failed to address security concerns associated with e-mail. ..... Lynn McNulty, NIST's associate director for computer security and a member of the board, said the board may recommend that the Office of Management and Budget institute the proper policy-making process 'so people like Tom have guidance to go by.' ..... Al Williams, acting director of GSA's Center for Infrastructure Security management, said he briefed the board a few hours after DeWitt's presentation. He assured members that his office would seriously address security issues associated with the governmentwide e-mail project as well those pertaining to electronic commerce and other services. Williams is slated to head GSA's new Infrastructure Security Program Management Office when the agency's reorganization is completed."

Brewin, Bob, "DoD releases strategy for global network," *Federal Computer Week*, Volume 9, Number 5, Page 1, March 6, 1995.

KEYWORDS: DISN

ABSTRACT: "Defense Information Systems Agency last week released its long-awaited program strategy for the next-generation global Defense Department network, and industry sources characterized it as broad in scope but short on detail.

DISN Program Strategy Highlights:

- DISA plans evolutionary development of new network.
- Envisioned as DISA-operated and managed running on DoD-owned switches with pipes acquired competitively, Network will evolve to a wideband Sonet infrastructure, running on ATM switches.
- Calls for separate voice and video contracts to replace AT&T DCTN contract that expires in February 1996.
- New contracts to include DISA support contract for a number of services and transmission capacity as well as a DISN support contract..

.....evolutionary, multiple-pathed approach that will take maximum advantage of installed government infrastructure, industry's capabilities and evolving technologies, ... DISN, according to the strategy document, will evolve into a global mega-network capable of handling voice and high bandwidth data such as imagery. It will also serve as the primary carrier for all value-added services provided under DoD programs, such as the Defense Message System, the global command and control system and electronic commerce/electronic data interchange related capabilities.' ..... The strategy paper also strongly indicated that DoD intends to use these contract vehicles to build its own network rather than opting for what the marketplace can provide. ..... DISA envisions using DoD-owned voice office switches in the continental United States and worldwide as the keystone of its own interim network ..... DISA intends to bundle circuits and transmission requirements at the base level. ..... This includes what the strategy document called a DISA Support contract ..... These services include voice, video and dedicated channels, plus administration of switched data and wireless service contracts. DISA also intends to run a separate procurement for video teleconferencing when the DCTN follow-on expires ..... DISA expects to end up with a Synchronous Optical Network running on advanced Asynchronous Transfer Mode switches and has already issued a request for information on both. ..... DISA also intends to retain control of DISN program management, the strategy document said, indicating any role a system integrator will play will be subordinate to the agency. "

Brewin, Bob; "Naval Academy Network Stung by Hacker Attack," *Federal Computer Week*, Vol. 9, No. 2, Page 3, January 23, 1995.

KEY WORDS: hacker, CERT

ABSTRACT: "Friday, Jan. 13....Naval Academy Data Network....Shut down the network to defend it from what the Navy called an 'intruder' who had installed password-sniffing software....Serves close to 4,000 midshipmen as well as faculty....Intruder installed the sniffer software on 'five or six' Sun Microsystems Inc. SPARC 2 workstations on the network....Sources familiar with the academy break-in said it was worse than Giannotti admitted. 'This was a really nasty attack....They got into 24 servers and put sniffer software on eight of them. It will probably be another two weeks before the academy network is completely restored,' a source said....At this time, the academy cannot determine whether the intruder actually captured any passwords with the software 'since the process was passive when we discovered it.'...The academy called in the Navy Computer Emergency Response Team....The academy has not yet determined whether the intruder used its system as a launch pad into other DoD or Federal systems, Giannotti said....Naval Academy attack shows the hackers have not gone away....Warren Suss...The government is staking its future efficiency on electronic benefits transfer and electronic commerce and, unless they can come up with an effective security solution, Federal networks are time bombs waiting to go off."

Brewin, Bob and Elizabeth Sikorovsky; "DISA Stings Uncover Computer Security Flaws," *Federal Computer Week*, Vol. 9, No. 3, Page 1, February 6, 1995.

KEYWORDS: DISA, hackers, DMS, budget, NSA, ASSIST, Infowar Protect

ABSTRACT: "Despite the severity of this problem -- and a sharp increase in attacks by real hackers against Pentagon computers -- internal National Security Agency documents obtained by FCW revealed that only one-quarter of the $705 million added to the DoD budget last year for information security has actually been used for that purpose. The majority of the funds instead were siphoned off to build the Defense Message System (DMS) Infrastructure. Commenting on the DoD attacks, Mike Higgins, chief of DISA's INFOSEC Countermeasures

Department...But despite this harsh lesson in what Higgins calls 'Infowar Protect,' tens of thousands of DoD unclassified-but-sensitive computer systems continue to experience hacker attacks that increase in both sophistication and frequency. We saw 255 attacks last year, and it will probably double this year....Software tools used in last week's attacks included what Higgins described as 'sweeper' software, which scans thousands of computers at a time, looking for one soft point....Paige allocated $392.7 million of those extra funds to DMS while providing only $24.9 million to Infowar Protect over a five-year period. Amounts ranged from a low of $2 million in 1996 and 1997 to $7 million in 2000 and 2001....Higgins did say that DISA's front-line defensive organization -- the Automated Systems Security Incident Support Team (ASSIST) -- currently only operates 17 hours a day but has received authorization to expand its personnel from 17 members to 36 and operate on a 24-hour-a-day basis....But, Higgins added, protecting Pentagon computers attached to the Internet is an exercise akin 'to making sure all the windows and doors in the Pentagon are locked."

"Budget Plan Leaves Military Computers Vulnerable to Intrusion. (Increased Funding Deemed Necessary to Improve Security on Computer Systems)," *Defense Daily*, Vol. 184, No. 54, Page 423 (3), September 16, 1994.

KEY WORDS: DISA, NSA, Paige, Deutch, budget options

ABSTRACT: "DoD's two top information systems officials, in a letter this summer, paint a dire picture of essential Pentagon information systems vulnerability. In the June 14 letter, Lt. Gen. Alonzo Short, then-director of DISA, and Vice Adm, J.M. McConnell, NSA director, describe the current situation: 'unknown intruders have repeatedly shown how easy it is to penetrate and gain control of computers upon which the Department's activities depends, including finance, R&D (research and development), personnel, health, logistics and other support and sustainment functions.'...The letter was sent through Emmett Paige, Jr., assistant secretary of defense for command, control, communications and intelligence (C3I), to Deputy Defense Secretary John Deutch....Penetration of unclassified computer files containing logistics and other support data may not appear to threaten the military's ability to wage war....This data, however, lies at the heart of the nation's ability to mobilize its forces....The infrastructure underpinning U.S. forces, including logistics information and power grids, is 'fundamental to the national defense,' and industry source said." "*Alternative One. Funding would remain at the level laid out in the POM for DISSP....It won't provide funding to detect even limited attacks by individuals....Would also reduce by 50 percent the number of personnel assigned to DISA's CISS....*Alternative Two. It would add 'funds for the development of tools and techniques to counter the current class of individual attacks on the Department's computers and networks.'...It would accelerate a variety of initiatives to improve the protection of networks supporting DoD's classified and unclassified systems from attack. Funding to strengthen security standards, improve security practices and upgrade tools for the detection of limited attacks would also be provided. *Alternative Three. The limited information warfare option would fund the development of tools and techniques to provide an initial capability to restore new critical information services following an information warfare attack on the Defense Information Infrastructure by terrorist groups and nation-states. It would broaden security research and development, accelerate the development of security protective measures and accelerate the production of security countermeasures. *Alternative Four. This option would fund a comprehensive program to counter both 'current attacks and those initiatives over the next ten years, to include the protection, identification and recovery from information warfare attacks,' according to the letter."

"CTIA Fights Fraud with Donation to Secret Service," *Phillips Business Information's Washington Telecom News*, Page 1, April 17, 1995.

KEYWORDS: Secret Service, CTIA, Cellular, FCC, ITA

ABSTRACT: "Industry associations seeking improved or expanded action by government authorities that regulate or protect them are realizing that providing those authorities with tools that expedite their tasks pay larger returns than waiting for the problem to take care of itself. A case in point was last Wednesday's donation by the Cellular Telecommunications Industry Association (CTIA) Fraud Task Force of more than $50,000 in wireless testing equipment and technical assistance to the U.S. Secret Service. ..... The Secret Service is the primary Federal agency commissioned with investigating telephone and electronic fraud, ... CTIA already has assisted in the training of 6,000 law enforcement officers in tracking cellular fraud. ..... The Secret Service will be able to use the equipment not only to investigate and prosecute fraudulent cellular users, but also to find a back-door approach to catching drug dealers and others who use the phones to hide their illegal activities. ..... The donation, the first the Secret Service has ever accepted from the private sector, is the latest in a series of association gifts to government agencies to aid in expediting their tasks. The FCC continues to applaud the efforts of the Industrial Telephone Association (ITA), a coalition made up of the American Mobile Telecommunications Association, the Personal Communications Industry Association and others that recently supplied manpower, technical expertise and software to the FCC's Wireless Bureau, so that it could process a backlog of 45,000 spectrum applications."

Carney, Dan; "Cybercop Wages War on Crime," *Federal Computer Week*, Vol. 9, No. 3, Page 1, February 6, 1995.

KEYWORDS: DoS, Computer Crimes, phreakers

ABSTRACT: "Chief of the Justice Department's Computer Crimes Division?...Degree from Syracuse Law School....Charney heads the office that pursues computer criminals on several fronts: hacking, writing viruses, copying software illegally and 'normal' crimes in which computers contain vital evidence....array of equipment in his office...a dedicated computer that has an Internet connection, another computer that stores sensitive information, a third that is connected to DoJ's agency-wide network; a Clipper chip-equipped encryption device; and a secure, encrypted telephone that he uses to talk to the CIA and the National Security Agency....Changing technology not only provides new opportunities for criminals, it also makes it harder for DoJ to investigate some crimes...the move by telephone companies to digital service and switches can make it impossible to tap a single line to gather information for a case. In a highly publicized case, the department used a phone tap to intercept a computer data transmission for the first time when gathering evidence to prosecute the Masters of Deception 'phone phreakers' case. Phone phreakers are hackers who break into corporate PBXs to make calls, often international ones, on the victim's phone bill. In other cases, phreakers attack the phone company itself, taking control of its digital switches. The Legion of Doom claims to have been in a position to turn off all telephone service in the Southeastern United States when the Atlanta-based phreakers took control of the switches in that region....Copyright infringement of computer software is another area that has received a lot of attention, he said. The problems in this area are societal and need to be addressed on that level....Charney added that people do not view intellectual property in the same way they view physical property....A high-profile area where the department concentrates fewer resources is that of destructive programs such as worms and viruses. Charney said this is because it is extremely difficult to find the original author of the destructive programs, and most infections are accidental, he said. 'There are more and more cases of malicious programming,' Charney said. 'But in most cases [infection] wasn't a deliberate criminal act.' The agency recently prosecuted the author of a virus at Cornell University as well as an employee at General Dynamics who planted a 'time bomb' program in the company's computer."

Carney, Dan, "Agency steers toward info highway 'emergency lane', *Federal Computer Week*, Volume 9, Number 8, Page 18, April 10, 1995.

KEYWORDS: FEMA, NII, Internet

ABSTRACT: "The Federal Emergency Management Agency aims to stake out an 'emergency lane' for the information highway that would provide priority access to communications during emergencies. ..... the agency is depending on information technology to help it do more with less and to facilitate communications with state, local and private recovery officials, said Harvey Ryland, deputy director of FEMA. ..... One way FEMA plans to build its emergency information conduit is through the Internet, according to John Hwang, associate director of the information technology services directorate at FEMA. FEMA plans to use cellular, wireless radio and even microwave satellite links to connect to the network. ..... The agency's plan is to create hypertext links to other related Web servers so viewers can 'surf the Net' from one server to another, Goodman said. FEMA is adding those links now. Other related Web servers include California's Office of Emergency Services, the Army Corps of Engineers and the Small Business Administration. ..... FEMA plans to work with telecommunications vendors to work out a personal identification number-based system that would give emergency workers priority access."

Coia, David Alan, "'Hacker' hounds tax cheats, Arlington hits paychecks to settle bills," *The Washington Times,* Page C9, March 30, 1995.

KEYWORDS: Hacker, tax evasion

ABSTRACT: "Since July, the county Treasurer's Office has used computer sleuthing to find delinquent taxpayers and slap liens on their paychecks. In the first seven months more than 2,100 residents were hit, bringing in $400,932 in personal property taxes from those who hadn't paid on their cars, country Treasurer Francis O'Leary said. The process is simple: If a resident owes $200, the county orders the employer to send $200 from the person's pay. ..... At first, the collection effort -- known as the Lien Machine -- involved five full-time and two part-time Treasurer's Office employees. They collected $267,098 in the first four months. ..... But in January the office hired Andrew Klages -- 'a computer hacker with an attitude,' Mr. O-Leary said -- at an annual salary of about $35,000."

"Computer Systems Security Exchange to Serve Industry, Federal Government," *Businesswire (BUSW)*, August 24, 1994.

KEY WORDS: Computer Sciences Corp., National Computer Security Association, National INFOSEC Exchange

ABSTRACT: "Computer Sciences Corp. and the National Computer Security Association (NCSA) have joined forces to launch a program to promote the open exchange of system-security information among private industry and the Federal government....The program will be called INFOSEC Technology Repository. The repository 'will contain lessons learned, vendor information, current and anticipated products, and information vital to both industry and government on information-security topics and issues.'...Other planned exchange offerings are technology forums and security conferences including targeted programs to assist academia in developing and introducing college-level information-security courses and special-interest groups to address specific and real-world information-security....National Computer Security Association....Paul Gates, NCSA membership chairman, at 717/258-1816, or fax 717/243-8642." "CONTACT: Computer Sciences Corp., El Segundo, Bill Lackey or Mary Rhodes, 310/615-0311."

Constance, Paul, "DoD brass at odds on how to boost security," *Government Computer News*, Volume 14, Number 8, Page 3, April 17, 1995.

KEYWORDS: DoD, INFOSEC, MLS

ABSTRACT: "As Pentagon brass approach a consensus on the need to bolster information security, long-standing disagreements over how best to protect military systems and networks surface. ..... Lt.Gen. Carl O'Berry, Air Force, deputy chief of staff for command, control, communications and computers, described MLS as 'a brain-dead idea based on the assumption that you can take responsibility for information security off the shoulders of man and put it in a machine.' ..... Lt.Gen. Albert Edmonds, director ..... DISA detects an average 1.5 attempted break-ins on its networks every day, according to Edmonds. 'Those are just the one we know about,' he said. Technical sophistication of electronic intruders is rising on a steep curve, Edmonds said, ... Point solutions to the security problems are plentiful, he said, but only complete departmentwide network solutions will achieve long-term security. ..... O'Berry said he would like to see a simplified approach to information security that focuses on three areas: data transmission, authentication of users, and risk assessment of the transmitted data."

Corcoran, Elizabeth; "Group Warns of Interlopers on Internet," *Washington Post*, Page D1, January 24, 1994.

KEYWORDS: Internet, firewall, CERT, spoofing

ABSTRACT: "Computer intruders are using a new technique for sneaking into computer networks, even those that already use 'fire walls' designed to keep out trespassers....The number of individuals and entrepreneurs eager to tap into the Internet has grown, so has the volume of users vulnerable to such intrusions....In the current infiltration scheme, the invading computer slips into a network by 'spoofing,' or fooling the network into thinking that it is a local computer. It does this by mimicking the identification of another computer that has easy access to the network. Once in a network, the marauding computer may 'hijack' the system by seizing a network connection already secured by a friendly computer. In this way, the intruding computer can bypass passwords and other protection schemes. From inside the network, the interloper can do anything an authorized user can do -- including change files....Local experts were divided about how pervasive such violations might be, but they were unanimous in saying that most computers making use of the Internet lack even the most rudimentary protection....For instance, one 'fire wall' security technique relies on using filters on routers -- computers that act as switches....But routers are the most vulnerable element in the Internet."

"Corporate America's Computer Data Continues to Be at Risk," *Business Wire*, November 15, 1994.

KEY WORDS: computer crimes, threat, Internet

ABSTRACT: "The risk to America's computer data continues to rise....Nine in ten (91 percent) information security managers surveyed report that corporations now face an increased security risk....An increase from last year's survey, when 80 percent of the respondents said that their corporate data was at risk....The threat of unauthorized access via the Internet was cited as a risk by over half (53 percent) of the respondents....Over half (55 percent) of those surveyed do not have any Internet security in place....Over one in ten (11 percent) of the respondents reported significant financial losses (including a number of losses in excess of $100,000)....Most significant threats to an organization are disgruntled ex-employees (95 percent), E-mail breaches (92 percent), hackers and unauthorized outsiders (91 percent) and unauthorized dial-up access (83 percent)....82 percent, of survey managers named PBX fraud as a security threat....Most significant impediments cited by respondents to providing computer security were an insufficient budget (55 percent) and senior management's lack of concern about security issues, as compared to other IT priorities....Most organizations do not understand the risks of neglecting security issues....Best solution. Almost half (49 percent) of the security managers surveyed report the best solution for their organization's network security is use of smart card-based one-time passwords. Only 22 percent report encryption of files, 16 percent report audit trails of system use and 13 percent report reusable passwords as the best solutions....Senior management lacks understanding. Over half (56 percent) of security managers give negative ratings to their senior management's understanding of security issues -- 45 percent say senior management has an 'only fair' understanding, another 11 percent give a 'poor' rating....Their executive management can potentially be held liable for losses resulting from network breach....CONTACT: Security Dynamics, David Hammond, 617/547-7820 or Schwartz Communications, Dana Harris/Mike Farber, 617/431-0770."

"Cryptography Export Control Costs U.S., Helps Competition *Signal*, Vol. 49, No. 2, Page 35, October 1994.

KEYWORDS: DES, NIST, Export control

ABSTRACT: "A worldwide survey of encryption products reveals that more than 400 products are available overseas. Many of these items incorporate the digital encryption standard and can be shipped into the United States from abroad. U.S. vendors, however, are not permitted to export products overseas with the digital encryption standard (DES). Most products from U.S. industry have DES or an equivalent public encryption capability. This is a major issue within the Clinton administration, because export control legislation is pending in Congress with revisions that could relax export of cryptography....Trusted Information Systems and the Software Publishers Association are continuing a joint year-long survey of encryption products, identifying the cryptographic technology involved in each country and its impact on U.S. industry. The data from the survey will be shared with NSA....The DES has been published openly as a Federal information processing standard (FIPS) by the government since 1977. Implementations of it in hardware and software routinely are available in the United States and throughout the world. Publication of software programs containing DES in paper form is permitted, but export as hardware and software is subject to government controls....The National Institute of Standards and Technology (NIST) recently published a FIPS processing standard that contained lines of source code for DES. In paper form, the automated password generation standard, FIPS 181, is acceptable for worldwide dissemination. When NIST recently made FIPS available over Internet, without export restriction notice, it immediately was copied by computers in Denmark, the United Kingdom and Taiwan....Now FIPS 181 is available from hosts throughout the world along with the notice that export of the technology from the United States is in violation of control laws.

"DataCop 2001: The Integrated Officer," *Washington Technology*, Vol. 9, No. 18, Page 16, December 22, 1994, TechNews, Inc.

KEYWORDS: Law enforcement, Clipper, crime

ABSTRACT: "High tech interest and money now found in law enforcement market, not DoD. Nation trying to get tough on crime. Technologies being explored include high speed networks for review of digitized fingerprints, hypertext links to photos, psychological makeup, credit information, mortgage information, IRA information, etc. Also facial recognition systems, neural networks for pattern recognition, infrared 'aura,' digital cameras, digital enhancement of photos and videos, and vehicle tracking. Down-side is privacy and vulnerability of 'evidence' to manipulation and change. Clipper chip being sidestepped with publicly available, largely uncrackable encryption techniques."

"Data Security," *Information Week*, Page 42, November 28, 1994.

KEYWORDS: Security, survey, comments

ABSTRACT: "..... scores of participants lashed out at their organization's attitude on a range of security issues .... Users are a problem. They don't want to be bothered with security.' .... 'If security gets too tight, people will circumvent it by writing passwords in plain sight or disconnecting security software.' .... 'Continued downsizing forces increased workload on those of us who are 'fortunate' to be employed here.' .... 'It's a classic dilemma -- good security leads to no events, which in turn causes management to cut the security budget.' "

Davis, Beth; "Raptor Expands Eagle's Wings," *Communications Week*, Page 66, March 27, 1995.

KEYWORDS: Firewall, encryption, industry, Internet

ABSTRACT: "Raptor Systems Inc. has announced upgrades to Eagle Enterprise, its Internet security firewall software. ..... Eagle Enterprise version 2.3 has a Microsoft Windows-based graphical user interface that makes it easier for network administrators to configure authorization rules, the company said. ..... Raptor also added Virtual Private Networking -- a capability that authenticates and encrypts traffic among multiple Internet sites within a company. Also, Eagle Enterprise 2.3 supports S/Key authentication, which provides one-time password authentication. Eagle Lite 1.0 offers many of the same features of the high-end Eagle Enterprise firewall but at a lower cost. It is designed for companies with 100 or fewer users. An add-on to Eagle Enterprise, Eagle Remote 1.0 is Internet-security software for companies with multiple corporate locations. Available now, Eagle Enterprise 2.3 is $25,000. A 50-user license for Eagle Lite 1.0 costs $7,500; a 100-user license is $12,500. Eagle

Remote 1.0 is $17,500. Both Eagle Lite and Eagle Remote will ship next quarter."

"Death of ITSSQC - A Retrograde Step?" *Computer Fraud and Security Bulletin*, September, 1994, Elsevier Advanced Technology Publications.

KEY WORDS: UK, Code of Practice, standards

ABSTRACT: "In the UK, the Department of Trade and Industry (DTI) has a prime aim in helping UK businesses to compete successfully at home and abroad....An example of a DTI effort in 'Good Practice' as it relates to the Quality/Security discipline is the DTI sponsored, 'A Code of Practice for Information Security Management' - BSI/DISC PD0003.) The DTI IT Standards, Security and Quality Committee (ITSSQC) reported within the ITAB structure and was responsible for recommending strategy and priorities within some significant 'soft infrastructure' areas....The Committee was formally disbanded in Spring 1994....ITSSQC consisted of a good cross section of IT practitioners from Finance, Industry, IT Vendors and Service Suppliers in addition to the professional DTI Secretariat....The loss of such an advisory body must have an adverse effect on 'soft infrastructure' disciplines."

de Borchgrave, Arnaud; "Russian Mobsters Loot U.S. Firms via Computer,", *The Washington Times,* February 6, 1995, page A1.

Keywords: Russia, international computer crime, theft, money laundering

Abstract: Russian crime gangs using economically desperate Russian computer scientists operating out of Moscow and St. Petersburg have launched attacks against U.S. corporations on behalf of transnational criminal organizations. Techniques used include "sniffers" and "trojan" horses to defeat electronic firewalls. These efforts seem to be justifying the predictions made by U.S. intelligence agencies over the last year. "Electronic attacks against company computer networks have sky-rocketed from 200 a year ago to almost 1000 a month." Forensics prove that the principal motivation is crime (theft, money laundering). "Computer rip-offs through the Internet last year topped an estimated $5 billion in the United States alone." Numbers of Russian crime gangs are growing dramatically and the FBI has identified over 200 operating in over 15 cities in a nearly like number of states. "Israel is so concerned about Russian money laundering that it has appointed a high-ranking Mossad official ... for the sole purpose of monitoring the traffic."

Dewar, Helen, "Regulatory Moratorium Is Blocked," *The Washington Post*, Page A1, March 29, 1995.

KEYWORDS: Regulatory, legislation

ABSTRACT: "The Senate yesterday scuttled a House-approved moratorium on new government regulations, clearing the way for approval today of a narrower bill that would give Congress powers to block regulations before they take effect. ..... The House would block issuance of most major new regulations until the end of the year or until a broader bill to curb unnecessary regulations is passed. By contrast, the Senate would put most new regulations on hold for 45 days to give Congress time to review and possibly overturn them. ..... The conflict between the two chambers is also evident in the Senate's broader regulatory bill, which would require agencies to conduct risk assessments and cost-benefit analyses of major regulations before they are issued. That bill would cover fewer rules than the House legislation and stops short of a House prohibition on regulations whose costs to industry are calculated to outweigh their benefits to society. ..... Sen. Don Nickles (R-Okla.) ..... agencies would have to send any rules with an economic impact of $100 million or more to Congress for review before they are put into effect. ..... While thousands of regulations will be subject to review every year, Nickles predicted that few would be over-ridden. 'But at least it would make Congress responsible,' he said."

Dibble, Julian; "Viruses Are Good for You," *Wired,* February 1995, page 126.

Keywords: Virus, Intelligent Agent

Overcoming a fear of viruses may be critical to the future of information - processing. Programmers such as Mark Ludwig and "Hellraiser" feel that viruses represent an advanced type of program necessary for application as intelligent agents.

"Digital Announces ChannelWorks Internet Brouter for Highspeed Internet Access Via Cable TV," *Pr Newswire (PRNW)*, July 25, 1994.

KEYWORDS: high bandwidth, cable TV, ChannelWorks, Internet

ABSTRACT: "Internet Brouter provides TCP/IP routing over cable TV systems and supports the simple network management protocol (SNMP) standard to facilitate smooth-running network operations and troubleshooting....6 MHz forward channel for outbound transmissions, and one 6 MHz reverse channel for inbound transmissions....$6,995."

"Digital Offers Data Network Extension," *South China Morning Post (SCMP)*, Page 5, August 30, 1994.

KEYWORDS: ChannelWorks, ATM, China

ABSTRACT: "ChannelWorks enables customers to extend broadband Ethernet local area network capabilities across television channels to any site on a cable TV network....ChannelWorks provides 10 megabits per second connectivity of Ethernet....Uses one forward and one reverse cable television channel, and can run alongside commercial programs....You can use SNMP to configure separate logical networks for different user groups - one for schools, one for hospitals, and one for businesses doing collaborative engineering, for example."

"DoD Ready to Hitchhike on the Info Highway (Department of Defense)," *Defense & Aerospace Electronics*, Vol. 4, No. 30, Page 1 (2), August 8, 1994.

KEY WORDS: information highway, NII, security

ABSTRACT: "'DoD has heard the message and definitely wants to ride the info superhighway into the future. But, this time it will be just another user,' a defense manager said. DoD will buy bandwidth on the system, just like any other user, and DoD's hardware and software will be off-the-shelf....DoD will add its expertise in specific areas, such as computers, communications and security....DoD is chairing the subcommittee on security....A strict user authentication process, effective user audit process, encryption of databases, and a standard accreditation process for security measures....As a NII user, DoD will not force the superhighway to go in any particular direction, and it doesn't want special treatment."

"Encryption: Business Group Recommends Specific Requirements for Encryption. (U.S. Council for International Business' Recommendations for Internationally Acceptable Systems)," *EDGE, On & About AT&T,* Vol. 9, No. 325, Page 1 (1), October 17, 1994.

KEY WORDS: associations, encryption, standard, policy

ABSTRACT: "The U.S. Council for International Business issued a statement Monday specifying requirements for encryption that should be incorporated into any internationally acceptable encryption system....U.S. Council recommends the removal of unnecessary export controls on commercial encryption products which hinder the ability of U.S. companies to compete. Also, many countries have a variety of restrictions, including import control laws and usage restrictions, which create an international environment that hinders business's ability to provide security for its worldwide communications....Business needs an internationally-accepted and comprehensive encryption policy. U.S. Council specified the following requirements....(1) free choice, (2) open to the public, (3) international acceptance, (4) flexibility of implementation, (5) user key management, (6) key escrow, and (7) liability....United States Council for International Business....It is Business and Industry Advisory Committee (BIAC) to the OECD."

Endoso, Joyce; "Commanders-in-Chief Need a Voice In IT Plans, Study Says," *Government Computer News,* Vol. 14, No. 2, Page 50, January 23, 1995, Cahners.

KEY WORDS: DSB, CINC's, DSCS

ABSTRACT: "Defense Science Board...Its December report, *Information Architecture for the Battlefield*, the board said the commanders-in-chief, known as CINCs, have gotten lost in the system development and modernization shuffle...The Defense Science board suggested the establishment of a new position for an information warfare officer who would build a strategic information warfare plan....The board's review also found that most information warfare technologies come from the commercial market....The board recommended moving the information load from Defense systems, such as the Defense Satellite Communications System, to commercial alternatives like satellite, fiber and wire technologies. The board also suggested that Defense Secretary William Perry create a Battlefield Information Task Force led by someone with sufficient command experience to win the CINCs' support. The task force should explore direct broadcast satellite service and use modeling for training and exercises, the report recommended."

"EU Promotes Infobahn - IT Superhighways," *Computing (CMPTNG),* Page 20, October 13, 1994.

KEYWORDS: information superhighways, telecommunications monopolies, regulatory, legal, G7, European Union

ABSTRACT: "The European Union has given top priority to the building of information superhighways in order to propel Europe into the fast lane of economic growth....According to "Georges Metakides, director of IT research and technical developments for the European Commission....G7 group to address it later this year....They will be seeking ways of implementing a G7 decision to encourage an integrated worldwide information infrastructure. For this electronic utopia to succeed, Metakides believes the protection of individual and business rights is vital. 'These include the protection of personal privacy, intellectual property rights, and information security on advanced electronic networks,' he explained."

"FCC Latest Target of Republican Downsizing Plan," *Phillips Business Information's Washington Telecom News*, Page 1, April 17, 1995

KEYWORDS: FCC, Downsizing, regulatory, Congress

ABSTRACT: The FCC's usefulness and very existence is under assault from Republican lawmakers and policy wonks, as both circulate plans around Washington with the intent of eventually abolishing the 61-year-old agency. It all started when House Telecommunications and Finance Subcommittee Chairman Jack Fields (R-Texas) revealed that he will deliver plans to the House Budget Committee that would reduce the agency's size and power. ..... Critics of the FCC now are focusing on the House because the Senate version of telecom-reform legislation does not include plans for restructuring the commission, a point that contributed to the opposition by Sens. John McCain (R-Ariz.) and Bob Packwood (R-Ore.). ..... McCain and Packwood later complained that Pressler's bill would instead increase the FCC's involvement in communications policy by providing it with 87 more regulations to enforce ..... cite delays in the deployment of cellular technologies, for example, that were introduced in the 1940's, but only reached market viability well into the 1980's after countless FCC deliberations. ..... Many plans circulating around Capitol Hill recommend that Congress decrease the FCC's funding so it would be forced to trim its own ranks."

"A Fire's Been Lit," *C4I News*, Vol. 2, No. 19, Phillips Business Information, Inc.

KEY WORDS: Comptroller, NSA

ABSTRACT: "Hamre is slated to discuss the information security budget with NSA Director Vice Adm. J.M. McConnell....Hamre's trip demonstrates he takes the warning seriously and could decide to boost information security spending, sources say."

"Future Navy Pub to Cover C2 Operations. (New Publication Entitles 'Naval Warfare') (Command, Control & Communications)," *Defense & Aerospace Electronics*, Vol. 4, No. 31, Page 4 (2), August 15, 1994.

KEY WORDS: Navy, policy, command and control, command and control warfare,

ABSTRACT: "Navy Doctrine Publication 1, 'Naval Warfare,' is the first of six planned publications, dispensing guidance for Navy and Marine Corps. The sixth volume, specifically on command and control, will provide the 'basic concepts to fulfill the information needs of commanders, forces and weapon systems....Information is not just a tool....Controlling information is the key to winning on the battlefield....When knowledge is military power."

Gallagher, Sean, Sam Masud, Joyce Endoso, Kevin Power, "BTG wins Air Force C2 Contract," *Government Computer News*, Volume 14, Number 1, page 4, Jan 9 95, Cahners Publishing Company, Newton, MA.

KEY WORDS: Air Force Information Warfare Center, BTG Inc., TBMS, Unix

ABSTRACT: "AFIWC awards five year $9.8 million contract to BTG Inc., Vienna, VA, 'to build intelligence and command-and-control applications for Unix platforms.'...Applications will run on Sun Microsystems Corp Sparc workstations running Sybase. BTG also has contract to develop Constant Source, an intelligence data display system. These applications will interface with TBMS."

"Getting Wired - Look Who's Talking - Security on Internet," *Computer Weekly (CMPWKY),* Page 48, December 1, 1994.

KEY WORDS: Internet's, OTA, firewalls, viruses, CERT, United Kingdom

ABSTRACT: "There are, however, well-established solutions now to all the main threats. For a general introduction to the area there is the consultative document RFC1244; alternatively, the recent report from the U.S. Office of Technology Assessment (OTA) is well worth obtaining (ftp://otabbs.ota.gov/pub/information.security/), while RFC1636 offers a more technical perspective....Four main areas of Internet security: unauthorized access, password management, viruses and encryption....A firewall is normally used to control unauthorized access....To join [a mailing list on firewalls] send the message subscribe firewalls to major domo greatcircle.com....The OTA suggests that you should 'treat your password like a toothbrush: use it every day, change it often, and never share it.'...Use anti-virus software....Information about viruses can be found from virus-I and valert-I. To join, send a message to listserv lehigh.edu with the message subscribe virus-I YourName or subscribe valert-I YourName respectively....Secure encryption techniques like PGP (Pretty Good Privacy) are now relatively widespread....A useful document about its activities at cert.org/pub/cert - faq. CERT has a Usenet newsgroup (comp.security.announce)....Comp.security.misc." is another."

Hauptman, Robert; "Add Ethics to the Agenda," *InformationWeek*, Page 64, February 6, 1995, Calmers Publishing Company.

KEY WORDS: Ethics, hackers, industrial espionage

ABSTRACT: "The really smart thieves do not bother with jewelry or silver or even cash. Now the major thefts take place in cyberspace....What we really need is an educational process on all levels that sensitizes those people who plan to work in the corporate sector to certain ethical foundations....There is no longer any doubt that both public networks and private systems are under fierce attack....It is the private systems that bring out the entrepreneurial spirit in sophisticated hackers. Here, the interest is in locating useful data and information including ideas that might lead to technological or marketing breakthroughs and thus, financial remuneration. Also highly prized are various passwords, codes, names, and numbers that allow hackers entry to the financial infrastructure....Imaginative films such as WarGames, Sneakers, and Disclosure have brought all of this to the public's attention."

"House Panel Begins Discussions on Post-FTS2000 Program," *Washington Telecom News*, Page 6, March 27, 1995.

KEYWORDS: Post-FTS2000, GAO

ABSTRACT: "Long-distance companies, regional holding companies (RHCs) and systems integrators testified last week before the House Subcommittee on Government Management, Information & Technology on the Federal government's Post-Federal Telecommunications System (Post-FTS2000) Acquisition Program. ..... According to Jack Brock, director of resources management at the General Accounting Office (GAO), the approach calls for 'two or more comprehensive service providers, one or more switched data and value-added service providers, two or more technical service providers to help user agencies apply telecommunications services and technologies to their missions, and a possible wireless communications service provider.' ..... He outlined eight issues that should be addressed before final requests for proposals are released in December. These include the issues of: mandatory use, program management, long-distance vs. local telecom services, packaging of services, interoperability, requirements, security and support for the National Information Infrastructure (NII).."

Houser, Walter R., "Tales from the Dark Side may replace I've Got a Secret," *Government Computer News*, Volume 14, Number 1, page 23, Jan 9 95, Cahners Publishing Company, Newton, MA.

KEY WORDS: Privacy, pending legislation, computer security, Freedom of Information Act, NII, World Wide Web

ABSTRACT: "Author relates various scenarios describing how private information, such as social security number, medical information, etc., might be available to unauthorized users and how it might be used. Nothing particularly new except that he identifies Chris Hibbert (hibbert@netcom.com) as a source of information on privacy and the social security number in /ftp/cprs/privacy/ssn on ftp.cprs.org and ftfm.mit.edu. He also says that these servers have directories of information on "pending legislation, privacy, the First Amendment, computer security, cryptography, the Freedom of Information Act, plans for the National Information Infrastructure, and Computer Professionals for Social Responsibility. Privacy-related World Wide Web pages are ftp://ftp.netcom.com/pub/agorics/hibbert/privacy.html."

"Industry, Government begin Development of Security Standards for NII," *Security Technology News*, Vol. 2, No. 15, July 29, 1994, Phillips Business Information, Inc.

KEY WORDS: standards, NII, interagency group

ABSTRACT: "A July 15 public meeting of the interagency Advisory Council on the NII....It's important for us to understand the needs for us to be able to respond, says Sally Katzen of the Office of Management and Budget, who chairs the Advisory Council....Subscribers to the NII must arrive at consensus on how to protect privacy, says Willis Ware of the Computer Systems Security & Privacy Advisory Board....On July 20, the American National Standards Institute convened 'a new panel to accelerate the development and acceptance of standards critical' to the NII. Both Peter McCloskey of the Electronic Industries Association and Peter Basserman of the Cellular Telecommunications Industry Association have asserted that market competition will generate NII standards."

"Information Security Losses Increasing at U.S. Corporations Says New Ernst & Young LLP and Information Week Survey," *Business Wire,* November 18, 1994.

KEY WORDS: survey, business, losses

ABSTRACT: "U.S. companies are experiencing an alarming increase in information security losses as they rapidly deploy new distributed computing technologies without taking proper security measures, according to a new survey study by Ernst & Young and Information Week magazine....Overall, 42 percent of respondents said senior management considered information security to be only 'somewhat important or not important.'...Based on 1,271 responses....More than one in every two respondents reported financial losses related to information security issues, sometimes exceeding $1 million....Those loss figures represent a significant increase over past estimates and indicate that companies are moving important business applications onto new systems without sufficiently planning for security.....Many organizations have no full-time resources devoted to information security (15 percent) or business continuity planning (25 percent). The greatest obstacles in addressing information security risks are reported as the following: lack of human resources (59 percent), budget (55 percent), management awareness (45 percent) and tools/solutions (42 percent)....Some 32 percent said they had experienced losses in the last two years, for which they could not provide a dollar amount. Some 17 percent said they had experienced losses ranging to $250,000 and 3 percent said their losses were between

$250,000 and $1 million....Seventeen respondents reported losses in excess of $1 million....The integrity and availability of information are currently reported as the top security objectives....Respondents indicated they were utilizing the following techniques: virus detection (91 percent), dial back or secure modems (54 percent), firewalls to protect from external access (45 percent), file encryption (36 percent), PC hardware security devices (33 percent), telecommunications encryption (22 percent) and message authorization codes (17 percent)."

"Information Warfare - Not a Paper War," *Journal of Electronic Defense*, Vol. 17, No. 8, Page 55, August, 1994.

KEY WORDS: Gulf War, information dominance, policy, MOP, information warfare, AFIWC

ABSTRACT: "As was obvious in the Iraqi conflict, we now live in the age of the electronic battlefield. Less obvious to many was the fact that we also live in an age where conflict of any kind creates a desperate need for huge volumes of information. The modern battlefield commander requires information as never before, and not just about enemy numbers, location, movements, readiness, weapons capabilities, control structures or awareness of friendly actions, but also about his own forces and allies. It has also become apparent that denying the enemy information about friendly forces is critical to the successful execution of a war, and protecting this information requires that you know yourself....In combat, however, the sources of this information do not usually arrive by the 'Information Superhighway.' More likely, the information flows over little used back roads that are important in combat but not always fully understood in peacetime. Interdicting, protecting and exploiting these information pathways is what IW is all about....*Knowledge*, defined separately from *information*, requires the processing, study and dissemination of a body of information and connotes an understanding of what is gathered....Disrupting vital command, information or supply lines can confuse an enemy's ability to understand what he is seeing until it is too late to take appropriate or effective action. Inserting erroneous information into the mosaic can create a false picture....Maj. Gen. Kenneth Minihan, the former commander of the Air Intelligence Agency, has stated that the objective is really 'Information Dominance.'...Command and Control Warfare...JCS Memorandum of Policy (MOP) 30 defines C^2W as 'The integrated use of OPSEC, military deception, PSYOPS, Electronic Warfare and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary capabilities, while protecting friendly capabilities against such actions.'...It also states the military strategy that implements Information Warfare....Air Intelligence Agency has created the Air Force Information Warfare Center (AFIWC)...the AFIWC was created through a merging of the Air Force Electronic Warfare Center and the security functions of the Air Force Cryptologic Support Center. This new center, located at Kelly

AFB in San Antonio, was activated on September 10, 1993....The IW Center develops, maintains and deploys C^{2}W capabilities in support of operations, campaign planning, acquisition and testing. Approximately 900 officers, enlisted personnel and civilians make up the AFIWC. There is a blend of operators (EWOs and pilots), scientists, engineers and intelligence specialists that creates a unique capability to examine carefully and support the many complex aspects of IW and C^{2}W....The AFIWC Operations Support Directorate maintains the ability to quickly deploy Information Warfare Support Teams to support combat operations....The AFIWC C^{2}W Database Director continually maintains select, critical databases to support combat operations, wargaming, testing and acquisition....The Systems Analysis Directorate provides quantitative analysis through modeling and simulation of offensive and defensive C^{2}W and IW capabilities....It examines new and emerging technologies for potential C^{2}W. W/IW applications and assists the Air Staff and major commands in developing C^{2}W requirements....The Engineering Analysis Directorate is responsible for improving the effectiveness of information, sensor and weapons systems for C^{2}W by providing technical support for U.S. and allied systems....Its Air Force Computer Emergency Response Team program provides 24-hour service for on-site consultation."

"JCS Vice Chairman Wants Information Warfare Improvements Faster," *Defense Daily*, Vol. 185, No. 24, Page 175, November 4, 1994.

KEY WORDS: reconnaissance, information warfare center, Joint Staff, policy

ABSTRACT: "There's a coming revolution in information warfare and military planners need to do a better job to prepare for it, Adm. William Owens, Vice Chairman of the Joint Chiefs of Staff, warned yesterday....I am not satisfied that we are doing as well as we could be, he told a symposium sponsored by the Center for Naval Analysis in Arlington, Va."

Jackson, William; "Commerce project time-outs put new chief in hot seat," *Government Computer News*, Page 65, March 6, 1995.

KEYWORDS: DoC, reorganization

ABSTRACT: "Alan P. Balutis, Commerce's director of budget, planning and organization, is taking over responsibility for the former offices of Information Policy, Information Planning and Review and Special Projects. ..... Patent and Trademark Office's Automated Patent System and the Advanced Weather Interactive Processing System at the National Weather Service. ..... That judging will be done largely by GSA, which controls the department's $20 million blanket delegation of procurement authority. The oversight invoked its Time-Out Program to resolve questions about APS and AWIPS."

Kerns, John M.; "Aviation Week & Space Technology," Vol. 141, No. 10, Page 17, September 5, 1994

KEY WORDS: DOT, Federal, executive departments, transportation

ABSTRACT: "John M. Kerns has become director of field operations for Counter Technology, Inc., Bethesda, Md. He was chief of the U.S. Transportation Dept.'s Personnel and Information Security Div.

Kniseley, Sina Fusco, "FinanceNet a Comprehensive Source," *Washington Technology*, Vol. 10, No. 25, Page 104, April 13, 1995

KEYWORDS: FinanceNet, NPR, WWW, NSF

ABSTRACT: "..... FinanceNet, a network designed to improve management of taxpayer resources and help agencies communicate with each other. The idea for the network came out of the National Performance Review's Financial Management Team, ... For the purpose of FinanceNet, financial management information is classified as OMB circulars, Government Accounting Office reports, and financial aspects of payroll and finance. ..... Many of the hyperlinks on FinanceNet's World Wide Web site lead the user to other comprehensive information sources, such as the Thomas Legislation site, FedWorld or the GAO. ..... While FinanceNet is an NPR initiative, it has taken on a life of its own, said B. Preston Rich, also co-chair of the core team. It is operated out of the National Science Foundation and Rich is the program director for FinanceNet as NSF. Funding is provided by the U.S. Chief Financial Officer Council, whose members include CFOs from 24 agencies. Each agency contributes $10,000 annually to FinanceNet, Rich said."

Marshall, Martin, "Oracle Bolsters Security," *CommunicationsWeek*, No. 554, Page 1, April 24, 1995.

KEY WORDS: Network security, client/server, database, ORACLE, Banyan, authentication

ABSTRACT: "With the new software, called Oracle Secure Network Services version 2.0, organizations will be able to add security features without having to revamp client/server applications, company officials said. It will be available in the second half of this year. ..... Secure Network Services will provide the foundation for a variety of third-party authentication schemes from Banyan Systems Inc., Bull Worldwide Information Systems, CyberSafe Corp., ICL Enterprises NA, Identix Inc. and Security Dynamics Technologies Inc. ..... Mark Jarvis, senior director of network products at Oracle, Redwood Shores, Calif. 'These third-party devices and software can add a whole new level of security without the corporate user having to rewrite his existing applications.'

..... The new version of Secure Network Services also will support centralized authentication servers based on Kerberos and Sesame technology. 'This will allow a user to have a single network log-in and to access, for example, 10 different Oracle databases across the enterprise,' Jarvis said. ..... This is made possible by having authentication services centralized in one server, rather than having each server perform its own authentication of every user, he said. ..... The Identix Touchsafe II Fingerprint Identity Verification Terminal relies upon the human fingerprint to ensure that only authorized personnel are allowed access to the appropriate network services. ..... The SecurID authentication scheme from Security Dynamics, Cambridge, Mass., relies on the company's smart-card technology. Each user is issued a card that changes the keycode on an LCD display every 60 seconds. The user reads that number, plus his Personal Identification Number to request access to the network. A single authentication server on the network knows what number should be displayed on the LCD panel of the user's smart card at any given movement. ..... Each of the four server-authentication software providers -- Banyan, Bull, CyberSafe and ICL -- has a scheme that operates somewhat differently. In Bull's Integrated System Management technology, user authentication is provided by passing an encrypted token to the server. If the server then needs to access another database, it becomes a client of the new server and passes the encrypted token to it. In this way, the environment can be heterogeneous -- consisting of PCs, Unix systems and mainframes, for example -- and still not require local database user management according to Bull, Waltham, Mass. The Kerberos-based Application Security Toolkit from CyberSafe, Redmond, Was., provides two authentication measures. It both performs an authentication of the user's identity and implements a mutual authentication between the user and the applications accessed by the user. ICL's Access Manager classifies users as belonging to certain roles or job types. The roles then automatically define the network services that will be authorized for that user, according to ICL, ... Banyan's implementation has none of the twists of the other three, but, like the others, it does offer a single log-on for access to multiple servers across the network, according to officials from Banyan, Westborough, Mass. ..... List prices vary from $200 to $6,000, depending upon network configuration."

Massari, Chester A.; "The Dynamics of Information Security (Department of Defense Technology is Being Transferred to Commercial Sector)," *Defense Electronics,* Vol. 26, No. 8, Page 16 (3), August, 1994.

KEY WORDS: technology transfer, cryptography, NIST, standards,

ABSTRACT: "The gap between military security technologies and commercial and industrial security needs is narrowing now that there is surplus production capacity for such technologies. The advent of the wireless world has placed a premium on protecting commercial and personal information....Paradigm shifts are occurring which will close the gap between evolving defense technologies and the commercial/industrial need for security....Cryptography consists of the encryption and decryption processes." "to make the information unintelligible to anyone who does not have the means (formula or algorithm and key) to decrypt the information." "Key: A variable is used to periodically change the algorithm....Key Distribution: The method of putting the periodic keys in the place they are needed when they are needed....Access Control: The processes and systems by which the person attempting electronic access to information is validated as being the person they claim to be (authentication)....Tamper protection: A series of processes, both electronic and physical, established to detect any attempts to physically intrude on electronic information or tamper with the security parameters....Recovery: built-in fail-safe features to prevent information loss or compromise....Technology Trends....A priority has been given to miniaturize the security features....Miniaturization has permitted the embedment of cryptographic features into the end items....As key distribution and other key management facilities are embedded into the host....The Use of Common Modules....A family of common modules is being incorporated by multiple defense contractors....Helps drive down the costs of the modules and increases their attractiveness for additional embedments, thus furthering the government's goal of proliferating security....In the realm of electronic key management, a similar miniaturization standardization process is occurring, albeit trailing by three or four years....Joint explorations of additional opportunities....The trend for miniaturization would naturally lead to software based solutions....The government, through the defense security suppliers, has created an educated supplier base for communications security technology. This facilitates the leveraging of industry's technical advances in directions complimentary with good security designs and practices....Commercial Electronic....Security Requirements....Countless initiatives are striving to bring effortless access to the wireless as well as the interactive wired world. However, access is a two-way street and the awareness of economic vulnerability is not maturing as fast as the technologies....Today we compete in a global arena where industrial espionage is considered an art form and where personnel, skilled in gathering information, advertise their services in the Wall Street Journal....There is excess industrial capacity for manufacturing the more exotic technologies required to make the electronic security available on a wider scale....A second reality is more and more legal battles are being fought over the protection of personal data, such as legal and medical records." "Defense Technology and Commercial Security Needs....This has led Harris to the conclusion that the elements of success can be quite transportable from defense based customers....*The system has to be designed to the highest protection level expected during the products lifetime....It is a responsibility of the security provider to apply expertise to users fundamental need. *Security vulnerability assessments, threat assessments, etc., should be carried out using the same methods developed for defense use....Effective, economical protection will be part of the electronics, not 'glued on' afterward. The methods used for the highest levels of security, that is for the nation's defense, are invaluable as a security *yardstick*....The National Institute of Standards and Technology (NIST) sets the standards for Federal (non-defense) applications, but they do not evaluate nor qualify any products, nor do they resolve any disputes or issues not pertaining to their standards."

Mayfield, W. Terry, "Computer and Information Systems Security Research Program," *Research Summaries,* Vol. 1, No. 2, Fall, 1994, Institute for Defense Analyses.

KEYWORDS: Trusted computer system, security architecture.

ABSTRACT: "IDA involved in computer and information systems security research since 1984. Support NSA, NCSC, USD(P), and DISA. Role includes establishing criteria for development of international standards, advise system developers, assist government in establishing technical requirements, and developing transition strategies and implementation plans for the DoD security architecture."

McAuliffe, Amy; "New Army Communications Procurement Begins to Crystallize (Battlefield Information Transport System Requirements)," *Defense Daily*, Vol. 185, No. 43, Page 321, December 6, 1994.

KEY WORDS: Army, BITS

ABSTRACT: "BITS, which the Army hopes can be developed by 1997, include integrated voice/data capability, one to four second speed of service and 100 Kilobits per second file transfer data throughput....Other BITS requirements include a range of 4 kilometers on-the-move and 10 km fixed. Technology demonstrations and evaluation of BITS are slated for the first quarter of FY '96.' "

McCarthy, Shawn P., "Build new spoofing barriers," *Government Computer News,* Page 44, February 20, 1995.

KEYWORDS: Spoofing, CERT, WAN

ABSTRACT: "No fooling -- protocol "spoofing" is a serious threat on wide area networks. An associated trend with potentially worse effects is the hijacking or takeover of terminals or even full Internet servers. ..... Details on such threats are listed in the Computer Emergency Response Team's advisory CA-95:01.IP, available via Internet anonymous File Transfer Protocol at *info.cert.org.* ..... The CERT advisory presents basic answers to attacks on routers. But there are other ways to beef up your security, particularly at an application gateway firewall. Raptor Systems Inc. of Waltham, Mass., recommends these basic security steps:

- Don't allow anyone root access to the computer that acts as your Internet gateway.
- Get software for the gateway computer that can be 'taught' which processes should be running. ..... Other methods include establishing a customized filtering router or building a filtering rule into the server, ..."

McCarthy, Shawn P., "Hey hackers! Secure Computing says you can't break into the Telnet site," *Government Computer News*, Volume 14, Number 1, Page 38, Jan 9 95, Cahners Publishing Company, Newton, MA.

KEY WORDS: firewall, dual use, hacker, Secure Computing, Sidewinder, DES

ABSTRACT: "Secure Computing Corp., Roseville, MN developed a firewall for DoD that will soon be available to other government networks. The Sidewinder system costs $30K which includes a 90 Mhz Pentium Unix sever and software. NSA will one of first users. Company invited hackers to try and break into a demo site. The system uses one-time passwords and challenge and password system using DES. Charlie Robertella (703-318-9188) is the company sales manager."

McCarthy, Shawn P., "Internet gatekeepers are more greeters than guardians," *Government Computer News,* Volume 14, Number 6, Page 63, March 20, 1995.

KEYWORDS: Internet, security, WWW, AOL

ABSTRACT: "The network gateway protection rule is this: If you don't know the identity of a client, don't grant an account. Federal Internet server managers should confirm the name, address and phone number (with call-back validation) of any person who holds an account. ..... The service causing the most security concern on the Internet these days is American Online Inc., Vienna, VA. AOL has a policy of handing out free software plus 10 hours of free time, ... AOL members can send Internet e-mail and visit other Internet sites via Gopher, WAIS and FTP tools. AOL reportedly will add World Wide Web access any day."

McCarthy, Shawn P., "Who's in charge of computer security? The feud goes on ...," *Government Computer News,* Volume 14, Number 7, Page 1, April 3, 1995.

KEYWORDS: INFOSEC, SPB

ABSTRACT: "Fearing a policy power grab, civilian agency security managers are challenging Defense Department efforts to regain clout in government information security. The Federal Computer Security Program Managers Forum has launched an unusually public campaign to prevent the new U.S. Security

Policy Board from redefining "national security-related information" and giving DoD officials more say in prescribing safeguards for unclassified systems operated by civilian agencies. ..... In a report detailing how the board should operate, the administration also called for an interagency subgroup, known as the Information Systems Security Committee (ISSC), to devise comprehensive data protection policies. ..... Sadie Pitcher, forum co-chair, urged the National Computer Systems Security and Privacy Advisory Board to issue a resolution denouncing this scheme as undermining the 1987 Computer Security Act. ..... Pitcher said the law explicitly prohibits DoD and intelligence agencies from playing anything more than a technical consultant's role in choosing security measures for civilian systems. Pitcher, the Commerce Department's information technology security manager, ... But Peter Saderholm, the Security Policy Board's staff director, defended the ISSC as a legitimate interagency group with ample civilian representation."

McCarthy, Shaw P., "Grab SATAN tool off the Net quickly to plug the holes in your networks," *Government Computer News,* Volume 14, Number 7, Page 6, April 3, 1995.

KEYWORDS: SATAN

ABSTRACT: "The Security Administrator Tool for Analyzing Networks (SATAN), one of the most comprehensive interfaces ever created to probe for network security holes, will be released freely this Wednesday on the Internet. ..... Farmer designed SATAN to automate scanning of vast network landscapes for open accounts and back doors. ..... The program, which runs on Sun Microsystems Inc., Silicon Graphics and other Unix platforms, can use virtually any Web browser. It also needs a copy of the Perl 5 scripting language for file-management tasks. SATAN Level 3 is scheduled for release April 5 on Internet server *ftp://ftp.lerc.nasa.gov/gov/security/* and at other sites such as *ftp.win.tue.nl* at the Eindhoven University of Technology in the Netherlands. Look in directory *pubs/security/* for the file SATAN.tar.z. Other servers are expected to post it soon thereafter."

McCarthy, Shawn P.; "Network break-ins reveal the chinks in systems security," *Government Computer News*, Page 63, August 8, 1994.

KEYWORDS: DoD, vulnerabilities, passwords, Unix, NIST

ABSTRACT: "Network administrators at a Texas Air Force base recently discovered they could crack about 70 percent of the passwords on their Unix network with tools resembling those now being used by Internet hackers. Working with a list of encrypted user passwords, the base administrators compared the passwords against a dictionary of encrypted words. Users who picked common words or proper names for their passwords 'failed' the test, said

Fred Rameras, a security expert at the Air Force Information Warfare Center in San Antonio, Texas. ..... Most Internet security breaches at government sites have been through Unix systems, which make up the majority of Internet hosts. But PC and Apple Macintosh networks have had Internet security problems, too, and password cracking can apply to any network. Rameras said his office has turned to programs called Crack and Security Profile Inspector, developed jointly by the Energy and Defense departments. They are available to Air Force systems managers from the Air Force Computer Emergency Response Team, tel. 210-977-3156. Other military administrators can contact the Defense Information Systems Agency's Center for Information Systems Security. ..... In some cases, it doesn't even take a known flaw to break in. when computers come out of the box configured with default Unix log-ons, a secondary problem arises in tracking the known security holes caused by the defaults, said Dennis Steinauer, supervisory computer scientist at the National Institute of Standards and Technology. 'Automated tests could turn up many of these problems,' Steinauer said. 'The tests could be done by the manufacturers to begin with -- the trick is to get them to help out.' He envisions 'a standard suite of tests for new computer systems. They could be certified, much like Energy Star systems are certified today.' ..... Other gaps arise from failing to close network accounts quickly when users leave, ignoring activity in old accounts and supporting more Internet functions than necessary. After a hacker was arrested recently by Britain's Scotland Yard for snooping around U.S. military networks, such warnings have taken on new urgency. The hacker broke into a network at Griffiss Air Force Base, N.Y., through a well-known security hole in the Unix Sendmail program. This happened despite alerts from the Pittsburgh-based Computer Emergency Response Team and postings on Internet mail lists telling administrators how to avoid Sendmail infiltration."

Menke, Susan, M., Power, Kevin, Jackson, William, and Masud, Sam, "Group wants security plan info," *Government Computer News,* Volume 14, Number 6, Page 5, March 20, 1995.

KEYWORDS: FOIA, Privacy, EPIC, PDD29, policy

ABSTRACT: "A Washington organization concerned about privacy has filed a Freedom of Information Act suit to obtain documents about President Clinton's classified directive that created a new Federal information security policy group. The Electronic Privacy Information Center (EPIC) is seeking copies of government reports related to Clinton's Presidential Decision Directive 29, which established the U.S. Security Policy Board to coordinate, develop and monitor security policy. ..... EPIC officials said they are concerned that the directive and related documents lay out plans for amending the 1987 Computer Security Act and crafting a new definition of 'national security-related information.' "

Messmer, Ellen; "Users Say Teamwork Is Key to Successful Net Security Plans," *Network World*, Vol. 11, No. 47, Pages 19, 24, November 21, 1994.

KEY WORDS: Computer Security Institute, fire wall, policy, layoffs, voluntary departures, human resources, disgruntled ex-employee

ABSTRACT: "According to security professionals who gathered at the Computer Security Institute's recent 21st Annual Computer Security Conference, a good way to build consensus is to pull together forums that meet regularly to address specific issues...Information security managers, computer-savvy technicians whose calling is to protect their organization's mainframe, PC and network resources, find their jobs often boil down to building the old team spirit. According to security professionals who gathered at the Computer Security Institute's 21st Annual Computer Security Conference here last week, a good way to build consensus is to pull together forums that meet regularly to address specific issues. The goal is to gain the confidence of everyone from the chief executive officer to network operations and human resources staff."

Minahan, Tim, "Intelligence Agencies Build Their Own Internet, With Security A Major Goal," *Government Computer News*, Volume 14, Number 1, Page 8, Jan 9 95, Cahners Publishing Company, Newton, MA.

KEY WORDS: Intelligence, Intelink, Internet, Unix, Mosaic, World Wide Web

ABSTRACT: "Intelink is a trusted Internet-like WAN linking NSA, CIA, and DoD and other U.S. security bureaus. Top Secret high network using Mosaic-like user interface tools and TCP/IP protocol. Multilevel security aspects still need to be worked out. DoD Intelligence will likely migrate to standard secure Unix systems....An Intelink panel is working with DISA to establish a common set of equipment for use by "crisis" operations teams."

Minahan, Tim, "U.S. can win with best IT, Gingrich says," *Government Computer News,* Volume 14, Number 4, Page 1, February 20, 1995.

KEYWORDS: Congress, IW, IT acquisition

ABSTRACT: "House Speaker Newt Gingrich (R-Ga.) and a fellow Republican, Sen. William S. Cohen of Maine, told audiences at the Armed Forces Communications and Electronics Association conference in Arlington, Va., that controlling information and the technologies that transmit it will be crucial to future military campaigns. ..... enemy's communications system, even for a matter of minutes, likely would dissuade that enemy from engaging in battle. ..... The House leader recommended development of a military-wide information intelligence system to integrate service systems and assess potential and actual military threats around the world. He said this system would help the president deal with potential hot spots before they flare up and provide the military with the information it needs to fight small wars. ..... But Cohen and Gingrich also warned that using IT could be just as devastating as it is helpful. 'Our reliance on information technology is a vulnerability as well as an asset,' Cohen said. ...... Gingrich added that Iraq would have been more effective in the Gulf War had it enlisted 20 hackers to dismantle commercial information systems in the United States. ..... Despite their endorsement for technology for the military, both lawmakers said the armed forces will not enjoy the full benefits of IT until the Federal acquisition process is overhauled."

Minahan, Tim; "NIST is a potential victim of GOP plan to eliminate four cabinet departments," *Government Computer News,* Page 60, March 6, 1995.

KEYWORDS: NIST, DoC, reorganization, NII

ABSTRACT: "Besides the departments of Energy, Education, and Housing and Urban Development, a group of Republican House members said they want to eliminate the Commerce Department, NIST's parent agency. ..... Ultimately, the fate of NIST's IT work -- establishing Federal Information Processing Standards, testing high-performance computing equipment, coordinating information security for civilian agencies and developing standards and applications for the National Information Infrastructure -- remains unknown, as yet. The work might be shifted to other departments and agencies, the GOP lawmakers suggested. ..... Rep. Dick Chrysler (R-Mich.), chairman of the Commerce task force, said that Commerce and its $3.6 billion budget is the 'golden goose' of the group's elimination efforts. ..... Chrysler said NIST was being studied now and that it was too early to tell what changes his task force will recommend. ..... added, the development of the NII should be left to private industry."

Minahan, Tim; "U.S. can win with bet IT, Gingrich says," *Government Computer News,* Vol. 14, No. 4, Page 1, February 20, 1995, Cahners Publication.

KEYWORDS: AFCEA, IW, acquisition

ABSTRACT: "Two Republican lawmakers this month briefed military and intelligence officers on strategies for harnessing information technology for modern warfare. House Speaker Newt Gingrich (R-Ga.) and a fellow Republican, Sen, William S. Cohen of Maine, told audiences at the Armed Forces Communications and Electronics Association conference in Arlington, Va. ..... 'The ability to disrupt the enemy's information flow will be one of the key factors of success on the battlefield,' Cohen said. ..... Gingrich said disabling an enemy's communications system, even for a matter of minutes, likely would dissuade that enemy from engaging in battle. The House leader recommended development of a military-wide information intelligence system to integrate service systems and assess potential and actual military threats around the world. ..... Gingrich also suggested using DoD's IT resources in other kinds of campaigns, such as anti-drug and anti-terrorism programs of Federal, state and local law enforcement. ..... Cohen and Gingrich also warned that using IT could be just as devastating as it is helpful. ..... 'Desert Storm networks could have been easily jammed had Saddam Hussein understood modern electronic warfare.' ..... Gingrich added that Iraq would have been more effective in the Gulf War had it enlisted 20 hackers to dismantle commercial information systems in the United States. ..... Both lawmakers said the armed forces will not enjoy the full benefits of IT until the Federal acquisition process is overhauled. Gingrich suggested the only way to develop a procurement system that will allow the Defense Department to 'maintain a generation's technology lead' is to trash the current process and replace it with a new model."

Mulqueen, John T., "Bankers See Internet As Risky Business," *Communications Week*, Page 1, April 10, 1995.

KEYWORDS: Internet, banking, encryption

ABSTRACT: "New York ..... Not only are networks vulnerable to hackers, but they also can be compromised by dishonest bank employees working alone or with conspirators, or by careless workers who inadvertently disclose passwords, said computer industry experts and other bankers speaking at a conference held two weeks ago at the Swiss Bank corporate center here. On top of that, encryption systems are so cumbersome to install and use that it will be difficult to build mass-market service around them, they said. ..... And encrypting credit card transactions over the Internet means merchants can become the target for hackers. ..... Martha Stansell-Gamm, the U.S. attorney who is prosecuting Kevin Mitnick, ... It is impossible to pinpoint the extent of computer or electronic criminal activity because there is no precise definition of it, and also because much of it is not reported, she said. ..... 'But the computer crime problem is getting worse,' ..... 'We are seeing more cases [of criminal activity] and the nature of the cases is getting more serious.' ..... Nathaniel Borenstein, chief scientist of First Virtual Corp., Santa Clara, Calif., ... If a bank uses encryption for commercial transactions, it might not be able to send those transactions across public networks in some countries, such as France, he said. Also, since there is no single standard for encryption, that limits interoperability with other banks or vendors that may use different encryption technology. ..... 'Properly managing private and public [encryption] keys is harder than setting the time on a VCR,' Borenstein said. ..... Daniel Schutzer, vice president and director of advanced technology at Citibank, admitted to the security shortcomings ..... Data on customers' transactions can be electronically integrated with the bank's accounting system to improve operations, he added. Physical protection is the best answer to security and will probably take the form of encrypted cards customers use on their computers to gain access to their accounts, he said. ..... The seminar was sponsored by the International Bank Study Center, an organization that studies banking issues, ..."

Munro, Neil, "Capital Round-up," *Washington Technology*, Vol. 9, No. 18, Page 8, December 22, 1994, TechNews, Inc.

KEYWORDS: DoC, FAA, USCG, GPS

ABSTRACT: "DoC panel recommends government use of 24-site FAA Wide Area Augmentation System and 73-site USCG Local Area Differential GPS for a highly accurate nationwide navigation network based on GPS."

Munro, Neil; "Congress Pushing for Telecom Reform," *Washington Technology*, Volume 9, Number 20, page 8, January 26, 1995.

KEY WORDS: Congress, telecommunications reform, commerce

ABSTRACT: "Congressional Republicans say they will push through a free-market telecommunications reform bill by July 4, and follow up by trying to open up the world telecommunications market....Long distance telephone companies, who charge the Republicans with drafting a bill too favorable to the seven locally dominant Baby Bells....Vice President Al Gore supports a semi-regulated competition. 'Without government intervention to break up monopolies, the free market may not yield a competitive market,' he said...Republicans differ; 'We should provide a competitive framework for business to work out its differences. The marketplace, not government, should pick the winners and losers,' Kansas Sen. Robert Dole, the Senate's new majority leader, said at a Jan. 9 Telecom hearing called by South Dakota republican Sen. Larry Pressler, the chairman of Senate Committee on Commerce, Science and Transportation....which is responsible for preparing the Senate's version of the telecom legislation....Make no mistake. The real problem in today's telecommunications industry is the monopoly local market, not the competitive long distance market, according to Howard Baker, chief lobbyist for the Competitive Long Distance Coalition, a Washington-based group that includes AT&T, Sprint and MCI....The Federal government should regulate narrowly [but] we cannot legislate in a vacuum, said Virginia Republican Rep. Thomas Bliley, chairman of the House Committee on Commerce....Our theme [is] to regulate only where necessary and to let market forces govern, said Texas Republican Rep. Jack Fields, chairman of the telecom panel in the House Committee on Commerce."

Munro, Neil, "New Info-War Doctrine Poses Risks, Gains" *Washington Technology*, Vol. 9, No. 18, Page 1, December 22, 1994, TechNews, Inc.

KEYWORDS: Presidential Review Decision, CIA, Clipper, DISA, power grid, banking

ABSTRACT: "We are not prepared for an electronic Pearl Harbor - Bob Ayers, CISS, DISA. Presidential Review Directive (Decision?) (PRD) being completed by EOP. CIA preparing a National Intelligence Estimate of possible threats. IW tools include deception, secrecy, electronic warfare, physical destruction, psychological warfare, intelligence. Services establishing IW centers. Intelligence agencies also pursuing. Weapons include airborne television studios, high-energy pulse weapons, and persistent computer viruses. IW is a two-edged sword - civilian distrust of Clipper chip deployment. DISA test of logistics and medical network vulnerabilities: attacked 9000 computers, hacked 88%, only 4% of successful attacks detected, only 5% of detections were reacted to. Banking industry in cooperation with Treasury Department has erected extensive defenses. Electrical power grid Supervising Control And Data Acquisition system also vulnerable. AT&T relies on multiple communications links, automated reaction to problems, and stringent protection of computerized switching stations. More interagency and government-industry cooperation needed - PRD may help. Legal problems - limited military role in protection of telephone network, no military role in protecting citizens from propaganda. Military has to make cultural adjustment of 'geeks' and their environment. Very precise intelligence data required. Current arsenal of IW weapons not suited to probable needs. COTS software is often vulnerable. Need career paths for Information Warriors."

Munro, Neil, "White House Security Panels Raise Hackles," *Washington Technology*, Page 6, February 23, 1995.

KEYWORDS: Security Policy Board, NII, PDD 29, INFOSEC, NIST

ABSTRACT: "A White House effort to coordinate security policy for the government's classified and unclassified information is sparking opposition from the same groups that stopped the stillborn Clipper chip initiative. The dispute will slow the formulation of a government-wide information protection plan, increasingly vital to both commerce and national security. ..... The Nov. 21 paper, titled 'Creating a New Order in U.S. Security Policy,' also called for creation of a new category of information dubbed national security related-information. Critics have two major concerns. The first is that government may be giving intelligence agencies unwarranted control over creating policy for unclassified information. ..... policy makers should not try to establish a common scheme for the protection of classified national security information, unclassified public-interest information, and private information held in the government's databases. ..... Hall said he hoped to see a single working group created to coordinate policies being created by the board and Vice President Al Gore's National Information Infrastructure Task Force. ..... The U.S. Security Policy Board was created and put under the control of the White House's National Security Council by Presidential Decision Directive 29. ..... Below the board is a larger 26-member Security Policy Forum composed of 26 representatives from many Federal agencies ..... Information systems security is 'the most difficult topic of all the ones I am working with,' said Saderholm. ..... But the obstacles facing the Security Policy Board are probably too great to overcome in the next two years, said sources. ..... Another likely flash point is the role of the National Institute for Standards and Technology, Gaithersburg, Md., which was given responsibility for protecting the government's unclassified data by the 1987 National Computer Security Act. ..... Pentagon officials working for Emmett Paige, the assistant secretary of defense for command, control, communications and intelligence, have drafted a Presidential Review Directive titled 'Policy on IW for Presidential Decision Directive,' but the policy document has not won final approval within the Pentagon, delaying its formal review by White House officials. ..... Jeffrey Smith."

Munro, Neil, "White House Security Panels Raise Hackles," *Federal Computer Week*, December 19, 1994.

KEYWORDS: Federal, SPB, unclassified information, national policy

ABSTRACT: "A White House effort to coordinate security policy for the government's classified and unclassified information is sparking opposition from the same groups that stopped the stillborn Clipper chip initiative. ..... Peter Saderholm, the board's secretary ..... papers prepared by the board, which outlined plans for the government-wide policy and urged revision of the National Computer Security Act of 1987. ..... The Nov. 21 paper, titled 'Creating a New Order in U.S. Security Policy,' also called for creation of a new category of information, dubbed national security related-information. Critics have two major concerns. The first is that government may be giving intelligence agencies unwarranted control over creating policy for unclassified information, said Steven Aftergood, an analyst for the Washington-based Federation of American Scientists. ..... He also believes policy makers should not try to establish a common scheme for the protection of classified national security information, unclassified public-interest information, and private information held in the government's databases. ..... Keith Hall, ... All decisions on security policy will be made by senior White House officials, he said. ..... The U.S. Security Policy Board was created and put under the control of the White House's National Security Council by Presidential Decision Directive 29. ..... But the obstacles facing the Security Policy Board are probably too great to overcome in the next two years, said sources. The controversy over the National Security Agency's Clipper chip may be a cautionary tale -- ..... Ultimately, opposition from privacy groups and the telecommunications industry derailed the chip, ... Industry officials successfully objected, saying the government-designed Clipper chip would be banned by foreign governments, crippling industry's plans for international sales and communications. ..... Many of these political issues have already crippled a more ambitious effort by the Pentagon to win White House approval for a national information warfare strategy, designed to protect military, Federal and commercial information systems from attacks during a war or crisis. ..... The information warfare strategy -- and security policy in general --raise many difficult technical, legal and even constitutional problems, said Jeffrey Smith, a Washington lawyer. ..... The basic question, he said, boils down to, 'What is the responsibility of government to protect its citizenry?' 'It's a hell of a problem [and is] much, much trickier' than the Clipper problem, he said."

"National Industrial Security Program Policy Advisory Committee," Vol. 59, No. 190, 59 FR 50257, October 3, 1994.

KEY WORDS: NISPPAC, NISP, ISOO

ABSTRACT: "Information Security Oversight Office....National Industrial Security Program Policy, Advisory Committee (NISPPAC). Date of Meeting: October 20, 1994....Information Security Oversight Office....To discuss National Industrial Security Program (NISP) policy matters....Steven Garfinkel, Director, ISSO, 750 17th Street, NW., Suite 530, Washington, DC 20006, telephone (202) 634-6150."

Nevin, Howard "Get secure in this brave new electronic world", *Government Computer News,* Volume 14, Number 7, Page 21, April 3, 1995.

KEYWORDS: Policy

ABSTRACT: "First, get educated. ..... Detechnify the issues and educate people in the real-world, commonsense issues and considerations. Second, define a practical security policy for the agency or the element you're concerned with. But consider the structure of the policy in layers: A technical and administrative layer would be fine for starters, and each can be subdivided or sublayered to meet the additional areas of concentration that may exist. ..... Third, then, you should broaden the focus anew and define a set of guidelines for physical security, operational security, etc. ..... Fourth, start planning your system based on the realities of existing technologies and products that support your overall security goals. ..... What you've done is to define the universe of products ..... that meet your practical computer/information security needs as they are currently established by policy or directive, and in the future based on applications and general system requirement."

"Overseas Hackers Force DoD to Revise System Security," *Government Computer News*, Vol. 13, No. 15, Page 8, July 18, 1994.

KEY WORDS: DISA, computer security, CERT, hackers, Europe

ABSTRACT: "Jan 1994, there have been at least 35 reports of illegal access and one person has been arrested in Europe. DoD officials say the 95% of the break-ins are due not to technical problems but to poor data security administration....Jim Christy, Air Force Office of Special Investigations....The Defense Information Systems Agency's Center for Information Systems Security now is studying the establishment of a military career track for computer security professionals. A CISS employee declined to give specifics....The number of attempts is increasing and so is the sophistication....After gaining superuser status on one system, a hacker can easily reset network interface cards to "promiscuous mode" to view data that passes through them. The hacker also can run a "sniffer" program to capture passwords and information and then "spoof" or imitate other users to enter more systems....Just 2 percent to 4 percent of such intrusions ever are detected."

Panettieri, Joseph C.; "New Net Threat," *InformationWeek*, Page 16, February 6, 1995, Calmers Publishing Company.

KEY WORDS: Internet, CERT, hackers, spoofing

ABSTRACT: "According to CERT, the Internet hackers use a technique called IP Spoofing that tricks a private network normally secure from external access into thinking a hacker is on the network as a legitimate user. To combat this method, organizations can use filtering software that neutralizes IP Spoofing, says Tom Longstaff, manager of research and development of CERT in Pittsburgh....Internet access provider Issue Dynamics Inc. in Washington...recently suffered network break-ins. According to Issue Dynamics president Sam Simon, CERT notified his firm in December that a hacker was posting pirated software on Issue's server. Moreover, the hacker was posting the company's encrypted password file on Internet newsgroups and using the server as what Simon calls 'an industrial espionage conduit' to spy on Net users....Attention to detail is the key, say experts."

Panettieri, Joseph C., "Are Your Computers Safe," *Information Week*, Page 34, November 28, 1994.

KEYWORDS: Internet, LAN/WAN security

ABSTRACT: "In fact, of the more than 1,250 participants in the second annual InformationWeek/Ernst & Young Information Security Survey, fewer than one in four technology managers considered information security to be extremely important. ..... 'Budget and staff shortages are way ahead of security worries at this time,' ..... The greatest obstacles to better data security? Lack of personnel, money, and tools -- and the apathy of top management. ..... 'Security staffs are expanding,' ..... By 1995, Motorola hopes to make every employee compliant with each of the company's desktop security rules. The rules include the use of boot protection, regular password updates, antivirus software, and screen lockouts that render a PC useless after 10 minutes of inactivity. ..... The company also uses data encryption across wide area networks (WANs), and an unspecified electronic-mail product that offers digital signature protection to verify user identity. ..... many deem the Internet insecure for business commerce because it is a distributed system with many access points that invite computer crime. ..... if the hackers had managed to shut down the weather network, all commercial airliners -- which depend on the center's forecasts -- would have been grounded. ..... Police in the United Kingdom only weeks ago arrested a 16-year-old who allegedly used his home computer to access the Internet and break into more than 100 international networks, including one that contains some explosive secrets: The (South) Korean Atomic Energy Research Institute (Kaeri). ..... reportedly made his connections through Griffiss Air Force Base in Rome, NY. ..... 'It's the insiders who know where and when to look,' says Daniel Geer, chief scientist at OpenVision Technologies Inc., a Pleasanton, Calif., developer of security software. ..... On Nov. 1, an MCI employee was charged with stealing 100,000 calling-card numbers that were later used to place $50 million worth of fraudulent calls. The employee ..... allegedly wrote software to capture card numbers from various carriers that used MCI's switching equipment. Lay, ... then sent the numbers to an international hacker ring ..... While conventional wisdom says the threat of computer viruses has diminished in recent years, survey respondents claim otherwise. ..... Conventional wisdom holds that larger computer systems are more secure. This time, at least, that seems on target."

Panettieri, Joseph C., "Infamous Hacker .....," *Information Week*, Page 14, March 13, 1995.

KEYWORDS: CERT, passwords, corporate security

ABSTRACT: "Petersen says technology managers would be well advised to read Internet security advisories released via electronic mail by the Computer Emergency Response Team (CERT) ... Petersen recommends the regular use of alpha-numeric passwords, rather than letter-only passwords .... 'Communication with employees is also key,' .....They should know not to answer questions posed by unfamiliar callers.'"

Pemberton, J. Michael, "RIM: Navigating Through a Maze of Associations. (Records and Information Management," *Records Management Quarterly*, Vol. 29, No. 4, Page 56 (3), October 1994.

KEY WORDS: Organizations, Associations

ABSTRACT: "Organizations that practice Records and Information Management should undertake cooperative endeavors with related professional groups to define the boundaries of the discipline. Thus, the American Records Management Association international should be interested in forging relationships with other associations. Some tips on how to explore useful relationships are presented....Ongoing shift in the larger social paradigm....Instead of depending, as we once did, on metaphors from physics (e.g., 'splitting,' 'atomic,' 'exploding'), we are using more biological expressions (i.e., 'adaptive,' 'integrative,' 'evolutionary'). Our sense of the new order is most clearly expressed, perhaps, in network terms (e.g., 'connectivity,' 'interface')....Associations focusing on information security consider the following bodies: The American Society for Industrial Security Business Espionage Controls and Countermeasures Association Business Systems Sales and Management Association Communications Security Association Computer Professionals for Social Responsibility Computer Security Institute Computer Virus Industry Association Data Processing Management Association Information Systems Security Association International Information Systems Security Certification Consortium National Association of Security and Data Vaults National Center for Computer Crime Data National Classification Management Society of Competitive Intelligence Professionals Association for Computing Machinery."

Pierce, Greg; "Reinvention of GSA necessary, says head," *Washington Times,* Page A-6, March 28, 1995.

KEYWORDS: Reorganization, Federal, GSA

ABSTRACT: "The head of the General Services Administration yesterday called his agency 'a troubled company,' and said reform efforts by the Clinton administration and Congress give employees a chance to recover their 'self-respect.' ..... The GSA, which handles government purchases and owns many Federal buildings, now has 16,611 employees, down from 20,660 when he took over the agency in 1993, Mr. Johnson said. By the end of the year, he said the total will fall to 15,514. 'So we'll be down 25 percent by the end of this year, without laying off a soul,' Mr. Johnson said."

Power, Kevin, "OMB to agencies: Secure your data, not just hardware," *Government Computer News,* Volume 14, Number 7, Page 53, April 3, 1995.

KEYWORDS: OMB, policy, NIST, DoJ

ABSTRACT: "The Office of Management and Budget has drafted new information security guidance that focuses on user behavior and risk management. ..... stresses individual responsibility, prescribes security controls for general support systems and urges agencies to integrate security programs with their mission goals. ..... Ed Springer, a desk officer in OMB's Office of Information and Regulatory Affairs, said the new A-130 security appendix focuses more on designing safeguards and rules that can handle the explosion in government networks and hold users accountable for their actions. ..... A-130 is the government's basic IT management policy document. OMB already has approved the revised sections dealing with information management policy and management practices for running IT systems. The security portion of A-130 recommends that agencies should develop access and behavior rules for all potential system users. These rules should cover a variety of circumstances including work-at-home programs, dial-in access, Internet connections, use of copyrighted software, and the unofficial use of government equipment. ..... 'The rules of behavior should be written down, with awareness and training programs built around those rules,' Springer said. ..... OMB reaffirmed the National Institute of Standards and Technology's role in developing civilian security standards and guidance. The new circular calls for the Justice Department to provide agencies with legal advice on reporting and handling security incidents, including working with law enforcement agencies. ..... OMB officials expect to issue a final version by fall. Meanwhile, Congress is set to begin hammering out a final version of an updated Paperwork Reduction Act. After years of dead ends, ... The Senate passed its version of the new act, S 244, in February. The House approved the counterpart legislation, HR 830, last month. ..... Most noticeably, the Senate bill steers clear of most references to information technology, while the House bill defines rules for handling information in electronic form."

Power, Kevin; "GSA Creates Security Office," *Government Computer News,* Vol. 14, No. 2, Page 55, January 23, 1995, A Cahners Publication.

KEY WORDS: GSA, NII Task Force, GITS, Information Security E-Mail, Digital Signatures

ABSTRACT: "Security Infrastructure Program Management Office is part of GSA's Office of full-time staff of program and technical experts borrowed from other agencies. Modeled after the Electronic Commerce Acquisition Team and Government wide E-Mail PMOs, the new office will work with other groups such as the National Information Infrastructure Task Force, National

Performance Review's Government Information Technology Working Group and Defense Department officials....Its goals, according to Jon Stairs, acting OIS chief, will be to develop an infrastructure for handling digital signatures and to identify methods for bolstering security in Federal electronic commerce and e-mail applications....We want to support and complement the electronic commerce and e-mail PMOs and make sure the security capabilities are in place for those applications....Deane Erwin, co-chairman of the Electronic Commerce PMO....Defense Information systems Agency, National Security Agency, Justice Department, Treasury Department and Postal Service have offered up to six full-time employees to staff the PMO." "PMO will take a government wide view and lay the security foundation for large-scale applications. Stairs also acknowledged that many policy and technical fights remain, especially on such controversial topics as rival digital signature algorithms and the key escrow encryption standard."

Power, Kevin; "NIST tackles next step; Actually using those digital signatures," *Government Computer News*, Vol. 13, Number 23, Page 1, October 17, 1994.

KEYWORDS: NIST, Digital signature

ABSTRACT: "The Digital Signature Standard takes effect Dec. 1, but most agencies likely will wait a year for the results of a National Institute Standards and Technology pilot before embarking on widespread use of digital signatures. ..... A NIST-sponsored interagency committee is developing an automated public-key infrastructure (PKI) pilot program. Represented on the committee are the National Security Agency, NASA, the General Services Administration, the Internal Revenue Service, the Education Department, the Social Security Administration and the Postal Service. To make digital signature use ubiquitous across government, NIST officials said, agencies must develop a public-key infrastructure as part of their larger information technology infrastructure. The NIST PKI pilot project will test management services, gauge digital signature tart-up costs and determine policy requirements, said F. Lynn McNulty, associate director for computer security at NIST's Computer Systems Laboratory. ..... At last week's annual National Computer Security Conference in Baltimore, NIST officials released the request for comments for the PKI pilot system, which is based on a study done for NIST by Mitre Corp. McNulty said NIST plans to issue a final request for proposals by January and award a contract around June. The pilot system should be running about six months later. ..... DSS is at the core of many of the National Performance Review initiatives for streamlining Federal operations and creating a government-wide electronic commerce system. ..... The standard is based on public-key cryptography techniques. This means users have both private keys, which are kept secret, and public keys, which can be known by anyone and are not altered. During the signature process, the sender first applies the government's Secure Hash Algorithm, prescribed by the Secure Hash Standard, to the message. This creates a shorter version of the message known as a message digest. The sender then applies his private key to the digest using mathematical procedures spelled out in the DSS Digital Signature Algorithm (DSA) to generate a specific digital signature. Anyone who has the sender's public key message and signature can verify the signature using the DSA. Verification shows that the message was signed by the public-key owner and was not modified after it was signed. ..... One security option proposed in the Mitre study calls for binding users with their keys in a digitally signed message, known as a certificate, and having it stamped by a trusted third party. These trusted or "certification authorities" would confirm the identity of users at the start of a transmission and issue message certificates along with public keys. ..... NIST officials have said they will be strict in their review of waiver applicants. Michael Rubin, NIST's deputy chief counsel, said an agency will have to show that DSS would prove too costly to use or would inhibit the agency's ability to carry out its mission. ..... Currently, IRS is considering a mixed scheme. The agency would use DSS for its internal messages, but use RSA applications for external communications, because many of its industry filers already use RSA encryption programs. Jim Robinette, the information systems security officer in IRS Systems Architecture Office, said IRS wants to avoid promulgating separate signature systems. ..... Some agencies have noted that NIST's pilot will not resolve some policy issues. The pilot does not deal with generation and oversight of private and public keys, McNulty acknowledged. ..... 'I think that's an issue that needs to be considered by the Government Information Technology Services Working Group,' McNulty said."

Power, Kevin, "Iowa will be the NII test bed," *Government Computer News,* Volume 2, Number 3, Page 1, March 1995.

KEYWORDS: NII

ABSTRACT: "Thanks to a congressional research grant, Iowa is gearing up to become the initial test bed for the national information super-highway. Congress recently approved a $3 million pilot project to explore ways to integrate and deliver Federal, state and local government services using the Iowa Communication Network (ICN). ..... ICN ..... is touted as the country's largest municipal synchronous optical network (Sonet). .....

Iowa to test 9 net apps with Uncle Sam

- A model Federal-state link ..... will give Iowa residents and businesses access to Federal data.
- A videoconferencing center ..... will be established to test telemedicine applications between VA medical centers and state hospitals.
- An access project will provide Internet links to selected schools, libraries and public organizations in southeast Iowa.
- Videoconferencing centers and gateways ..... to conduct claim hearings.

- A videoconference center ..... for video arraignments, parole board hearings and bankruptcy cases.
- A videoconference center ..... to conduct hearings with area veterans.
- For telemedicine tests, ICN access will be extended to include VA medical centers .....
- A videoconferencing center ..... to provide IRS training programs to area residents and businesses.
- ICN will be linked ..... to evaluate the nationwide impact of advanced network technologies."

Power, Kevin; "NIST plots new security plan," *Government Computer News*, Page 56, November 7, 1995.

KEYWORDS: NIST, Trust Technology, Assessment Program (TTAP)

ABSTRACT: "NIST officials already are trying to establish the Trust Technology Assessment Program. TTAP would involve certifying vendor and government laboratories that would provide faster, cheaper low-end security product ratings. The new initiative, however, calls for relying on vendors to abide by a grading process based on agreed upon product development standards and procedures. The assurance program would augment the TTAP initiative and possibly eliminate the need for testing some products targeted for lower-end security levels, said Pat Toth, a computer scientist in the Computer Security Planning and Assistance Group of NIST's Computer Systems Laboratory. ..... Through the TTAP plan, vendors would pay a fee to have products examined by accredited private and agency labs. ..... During a recent international workshop hosted by NIST, Toth said officials from Canada, Europe and Japan agreed that developmental assurance is a worthwhile goal. But officials also debated whether there was any reliable formula for gauging a vendor's development performance and integrating this new procedure into the emerging international security criteria, she said."

Power, Kevin; "Standards network links databases for quick retrieval," *Government Computer News*, Page 56, November 7, 1995.

KEYWORDS: NIST, National Standards System Network

ABSTRACT: "The National Institute of Standards and Technology and the American National Standards Institute predict that their National Standards System Network will help agencies and vendors reduce systems development costs. ..... The network, known as NSSN, will link databases around the world to allow the exchange of information about the production, development, distribution and use of technical standards. NIST officials said NSSN will use Internet gateways to tap into existing government and industry networks. The most attractive NSSN feature will be its ability to provide users with cataloguing, indexing, searching and routing capabilities to locate and retrieve standards materials, said Belinda Collins, acting director of NIST's Office of Standards Services. ..... To develop NSSN, NIST received $2 million from a grant from the government's Technology Reinvestment Program and contributions from ANSI members. ..... NIST officials said they want the network operational within five years. For the first phase of the project, NIST and ANSI will analyze user needs and define NSSN specifications. Next year, the two organizations plan to launch a prototype network and fine-tune the system requirements. The NSSN program is voluntary but because standards are so expensive to develop, NIST and ANSI officials expect widespread participation from agencies, companies, industry groups and libraries."

Reed, Anne F. Thompson, "USDA sets sights on sharing e-mail," *Government Computer News,* Page 18, October 17, 1994.

KEYWORDS: E-mail, Federal

ABSTRACT: "Although many users in the department have access to e-mail, there are several disparate systems running in the department, said John Okay, USDA's IRM director. 'Sharing e-mail is something we can't do today.' Early drafts for next year's e-mail project lay out plans for converting existing systems to X.400 capability. ..... In a separate mail project, the department wants to install an Internet gateway at its headquarters offices by year's end. The IRM Office has begun a project with their Procurement Office to launch a pilot electronic commerce project. ..... Okay said USDA is gearing up for a demonstration project this fall. Last year's executive order from President Clinton requires all agencies to develop EDI systems to handle procurements by 1997. The Office of Federal Procurement Policy is overseeing the program."

"Reinventing, Again," *Washington Times*, Page A-4, March 28, 1995.

KEYWORDS: Reorganization, Federal

ABSTRACT: "**National Aeronautics and Space Administration:** Restructure to conform with a $13 billion space program instead of the $20 billion program ..... More than 1,500 of its 23,000 civil service workers already have taken buyouts ..... another 500 are expected to follow. **Estimated savings:** $8 billion and 2,000 positions.
Interior Department: Eliminate the Minerals Management Service and transfer royalty collection duties to states and tribes. Eliminate the office that deals with U.S. territories. Accelerate the transfer of Bureau of Indian Affairs programs to tribes. Transfer three Washington-area highways to Maryland and Virginia. Allow current offshore oil and gas royalties to be purchased. **Estimated savings:** $3.8 billion and 2,000 positions.

Small Business Administration: Eliminate subsidies the government pays on loans, imposing fees on lenders and borrowers. Consolidate field offices. Move more programs from headquarters to less costly field offices. **Estimated savings:** $1.2 billion and 500 positions.
Federal Emergency Management Agency: Sign contracts with governors to reduce reporting requirements and make it easier to respond to disasters. Provide incentives to states to establish their own emergency funds. Require states to pay for uninsured public repairs equal to a deductible level established by the Federal government. **Estimated savings:** $100 million and 305 positions.
Federal Communications Commission: Raised $7.7 billion by auctioning broadcast frequencies for the new generation of mobile telephones. Until Congress gave it the authority, the agency gave away licenses to companies to use pieces of the public's airwaves. No positions eliminated."

Rendleman, John and Rockwell, Mark, "Telcos Take the Internet Plunge," *Communications Week,* Page 5, April 3, 1995.

KEYWORDS: Internet, WWW, RSA

ABSTRACT: "MCI ..... internetMCI ..... nationwide dial-up access at 28.8 kilobits ..... internetMCI package separately for $39.95. 'The software incorporates client and World Wide Web browser software by Netscape Communications Corp., Internet software from FTP Software Inc. and encryption technology from RSA Data Security Inc. ..... includes access to free news services, directories to national Internet addresses and news groups, telephone, directory information and an information desk. ..... Nationwide 800 access to the service is available now, with local access scheduled for 64 U.S. cities by late April,' MCI said. ' Customers will pay $19.95 a month for unlimited 800 or local Internet access between now and June 30,' MCI said. After June 30, users will pay $9.95 per month for five hours of local access and $2.50 per hour for additional hours, while 800 access will cost $6.50 per hour."

Rendleman, John, "CommerceNet Launches Pilot Internet-Security Program," *Communications Week*, Page 8, April 17, 1995.

KEYWORDS: CommerceNet, Internet

ABSTRACT: "CommerceNet, the consortium formed to promote electronic commerce on the Internet, last week launched a pilot program to certify the authorization and security of World Wide Web servers and Internet users. The program, called the Certification Authority pilot project, uses an authorization procedure and public-key encryption technology to certify secure Web servers and individual users doing business on the Internet, ... CommerceNet members will receive public-key certificates for secure Web servers from the CommerceNet Server Certification Authority, while individuals will get certificates from the consortium's Affiliated Individual Certification Authority. ..... Third-party verification of authorization and security will be necessary to establish the legitimacy of buyers and sellers on the Internet, one analyst said. 'The key is to have a credible third party,' ....."

Reynolds, Simon; "The Show Must Go On - Continuity Planning," *Corporate Cover (CORCOV),* Page 16, December 13, 1994.

KEYWORDS: continuity planning, disaster recovery, Code of Practice, United Kingdom

ABSTRACT: "Effective business continuity planning....Recognises that recovery of IT systems alone is not enough if all the elements required to carry on business (people, workspaces, plant, communication systems, documents et cetera) are not available in the right place at the right time....The Code of Practice for Information Security Management, published in September 1993, will become a British Standard, BS7799, early in 1995....Certification to an international standard within the ISO9000 series is widely accepted as demonstration of a commitment to quality assurance, for example, BS5750/ISO9000....The Code of Practice for Information Security Management states that the business continuity planning process should cover:

- Identification and prioritization of critical business processes.
- Determining the potential impact of various types of disaster, on business activities.
- Identifying and agreeing upon all responsibilities and emergency arrangements.
- Documentation of agreed procedures and processes.
- Education of staff.
- Testing the plans.
- Updating the plans."

Rockwell, Mark; "Telecom Reform Closer," *Communications Week,* Page 1, March 27, 1995.

KEYWORDS: Legislation, pending, telecommunication reform

ABSTRACT: "Fast-moving legislation that would revolutionize the U.S. telecommunications landscape took another important step forward here last week as the Senate Commerce Committee gave its stamp of approval. ..... Commerce Committee passed, with some changes, legislation introduced ..... that would overhaul the Communications Act of 1934. The bill would unshackle the local Bell companies from their long distance and manufacturing restrictions, free utility companies to provide telecommunications services, let telephone companies enter cable markets and cable companies cross over into telephone service markets, and modify cable and broadcast television rules. ..... The long distance industry's main objection seemed to be about which agency would enforce rules against anti-competitive behavior. Long distance providers would have preferred the Department of Justice, but the bill specifies the FCC for the task. ..... Local telephone companies, on the other hand, are concerned that 'date-certain' language in the original bill, giving them a set date when they could start providing long distance service, was replaced with a 'competitive checklist' of conditions that would have to be met before they could enter long distance markets. ..... The FCC would determine if a Bell company met the requirements."

Roeckl, Chris, "Taking Apps Security To the Next Level," *CommunicationsWeek*, No. 554, Page 3, April 24, 1995.

KEY WORDS: Client/server, database, security

ABSTRACT: "..... Most organizations, while embracing the concept of migrating computing resources closer to end users, have feared actually putting those key applications into the distributed-computing infrastructure. That's hardly a surprise given the lack of tools you need to secure these environments. The tools are readily available for mainframes, so why mess with success? ..... wrestling with what it means to secure a client/server environment. Is a network log-in enough, or are other tools required? The bottom line is most network and IS managers have a sense of the security problem, but remain uncertain as to the best way to solve it. ..... Oracle ..... announced new software and a third-party program aimed at securing the client/server database arena, ... With it, organizations create authentication servers that will let users log into many network databases using a single network log-in. ..... maintaining a single log-in to multiple databases is easier than maintaining passwords for every individual network database. Secure Network Services also will be the foundation for a variety of third-party security products."

Schwartz, John; "Chipping In to Curb Computer Crime;" *The Washington Post,* February 19, 1995, page A1.

KEY WORDS: Computer Break-Ins, Computer Crime Law Enforcement, Encryption Policy

ABSTRACT: Unusual collaboration between Federal law enforcement authorities led to arrest of Kevin Mitnick, the "most wanted computer hacker in the world." "The manhunt involved the FBI's National Computer Crime Squad in Washington, as well as FBI and U.S. Attorney's offices in Raleigh and Greensboro, N.C., San Diego, Los Angeles, San Francisco and Colorado," the San Diego Super Computing Center, independent consultants, and computer civil libertarian organizations. Mitnick disappeared in November 1992, having violated the terms of probation from a 1989 conviction for break-ins to Digital Equipment Corporation. Mitnick was pursued by Tsutomu Shimomura of the San Diego Super Computer Center who felt challenged by Mitnick's breaking into Shimomura's computer files of how to break into computer and cellular telephone networks. A Whole Earth Lectronic Link (WELL) based account belonging to Bruce Koball was found to contain files of electronic mail to Shimomora. Koball heads a civil libertarian organization called Computers, Freedom and Privacy. Shimomura has ties to a co-founder of the Electronic Frontier Foundation which has ties to WELL, as well as Computer Professionals for Social Responsibility, another civil libertarian organization. Terry McGillen of CERT says that break-ins only reflect the increased use of the Internet and nothing more. "In 1994, there were 2,241 incidents of unauthorized computer access involving some 40,000 machines reported to the Pittsburgh-based group." Encryption may be the solution, but the U.S. government continues to be concerned about widespread encryption use because of criminal use. Government also limits the export of encryption technology making it difficult to commercialize applications.

Schwartz, John, "Privacy Program: An On-Line Weapons? Inventor May Face Indictment for Encryption Software Sent Abroad," *The Washington Post*, Page A1, April 3, 1995.

KEYWORDS: Encryption, export, criminal

ABSTRACT: "Phillip Zimmermann ..... may be indicted ..... He created a powerful software program for scrambling information and communications on personal computers, and he distributed it free so that all computer users could have privacy protection. ..... after a friend put the program on the Internet, anyone around the world with a PC and modem could get a copy. That may constitute a violation of U.S. export laws, which classify encryption technology as powerful weapon whose export is strictly controlled. If the case ever comes to trial, a court will decide whether putting something on the Internet constitutes exporting it. Zimmermann said he wrote the software to help individuals guard their own privacy in an increasingly snoopy era. ..... If Zimmermann is indicated and convicted, he could be imprisoned up to five years and fined as much as $1 million. William P. Keane, the U.S. attorney in San Jose, Calif., has been investigating the case, and an indictment could follow. ..... Zimmermann said he also has a waiting list of lawyers offering pro bono representation. Lance J. Hoffman, a professor of computer science and author of a new book on cryptography controversies, said a Zimmermann prosecution 'would be the Dreyfus trial of this century' -- a landmark case for the culture of cyberspace. ..... One way the government has tried to address the widespread use of encryption is through stringent export regulations to control dissemination of such technologies. Those rules even apply to such garden-variety software as Norton Utilities, which offers encryption as part of its popular package of tools to help computer users manage their machines. ..... A Zimmermann indictment would be a disaster for the administration, said Jerry Berman, who heads the Center for Democracy and Technology, a high-tech policy group. ..... To Zimmermann, who was an anti-nuclear war activist in the 1980s, writing a crypto-for-the-masses project was just another form of social activism. He began writing the program in 1986, fiddling with it from time to time. ..... By mid-1991, he had a workable program. Zimmermann named it Pretty Good Privacy (PGP), after Ralph's Pretty Good Grocery in Garrison Keillor's mythical Lake Wobegon. He gave it to friends. ..... But then a friend put the program on a computer in the United States ..... Zimmermann knows that his brainchild can be used by criminals, and law enforcement officials bemoan the fact that they could not read an arrested pedophile's PGP-encrypted computer records. 'It's terrible to hear about cases like that,' said Zimmermann, who has two young daughters. But he contends that his product, which is now available in a commercial version from Phoenix-based ViaCrypt, is just 'a tool' that can be used for good or evil. ..... U.S. Attorney Keane said the case raises several questions: 'What -- if any -- policing is to be done on the 'Net? Are we going to throw up our hands and say 'There's no accountability. It's too big to enforce?' It's not our responsibility to determine whether a particular law is good or not,' Keane said. 'It's only our responsibility to determine whether a particular law applies, or should apply, in a given case.' But the encryption genie is already out of the bottle, industry executives argue, and the government's restrictions needlessly hamstring American companies. 'If the export controls are supported to stem the spread of this technology, it's not working,' said Doug Miller, government affairs manager for the Software Publishers Association (SPA). An SPA study found 400 encryption products readily available overseas -- including 164 that use encryption methods that the U.S. government has declared illegal to export."

"Secrets Safe with CardSecrets," *Government Computer News,* Volume 14, Number 3, February 6, 1995, page 3.

KEYWORDS: Public-key encryption, file security

ABSTRACT: "A $250 card is now available to secure files and communications for mobile and desktop PCs using access control, encryption, digital signature, and authentication techniques. The card complies with FIPS 140-1 and can incorporate any of the following encryption schemes: Elliptic Curve and RSA Data Security, Inc. public-key and DES."

"Security, Encryption Suits Filed," *Washington Technology,* Page 8, March 23, 1995.

KEYWORDS: EPIC, SPB, EFF

ABSTRACT: "The Washington-based Electronic Privacy Information Center has asked the courts to force the release of documents prepared by the White House's Security Policy Board. ..... Also, the Washington-based branch of another electronic-privacy group, the Electronic Frontier Foundation, recently petitioned the courts to outlaw controls on encryption technology as a violation of the Constitution's freedom of speech provisions."

"Senate Plans Early Hearings of Internet Use by Federal Agencies," *Washington Telecom News*, Vol. 2, No. 42, Page 1 (3), October 24, 1994.

KEY WORDS: Laws, regulations, congressional inquiries, Computer Security Act of 1985, OTA, hackers, FBI, IRS, Internet, cryptography policy, key-escrow

ABSTRACT: "A Senate committee on government operations is concerned that some networks such as Internet could already be targets of computer abusers....Sen. William Roth Jr. (R-Del.), ranking minority member on the Senate Government Affairs Committee, has told colleagues he plans hearings that could bring updated security amendments to the now-aging Computer Security Act of 1985."

"Services Gear Up for Information War," *Defense Daily,* Vol. 184, No. 48, Page 377, September 8, 1994.

KEY WORDS: services, information warfare, Navy, NIWA, Army, Air Force, AFIWC, J-3, JEWC, JC2WC, DSB, directive, Policy

ABSTRACT: "The Navy, for instance, last month announced the formation of the Navy Information Warfare Activity (NIWA). NIWA, which represents a redirection of the existing Naval Security Group Command, will examine information warfare capabilities essential for future conflicts. The Army is soon expected to stand up a new information warfare organization, to be located at Ft. Belvoir, VA....The Army's information warfare activities are primarily located in the Intelligence and Security Command at
Ft. Belvoir, as well as the office of the deputy chief of staff for operations and plans....The new Army organization is expected to focus on offensive missions....The Army's plans are in line with the emphasis Chief of Staff Gen. Gordon Sullivan has placed on information warfare and the digital battlefield....October 1993 Air Force information warfare restructuring, which redesignated the Air Force Intelligence Command the Air Intelligence Agency. The Air Intelligence Agency, located at Kelly AFB, Texas, encompasses the Air Force Information Warfare Center. Also located at the base is a distinct

organization, the Electronic Warfare Center, led by the Joint Chiefs of Staff....A draft Defense Science Board study completed over the summer, Information Architecture for the Battlefield, recommends that DoD put increasing emphasis on, as well as dedicate more funding to, information warfare."

Sikorovsky, Elizabeth; "Changes Open Fed Computers to Attack," *Federal Computer Week*, Vol. 9, No. 2, Page 8, January 23, 1995.

KEY WORDS: Computer Fraud and Abuse Act, Justice Department

ABSTRACT: "Federal officials are scrambling to plug holes in the Computer Fraud and Abuse Act, where recent changes have stripped away language protecting some Federal and financial computer systems from hacking. Those changes, made last year during the passage of the Crime Bill, cut language that prohibits unauthorized access, alteration or damage to 'Federal interest' computers. The new language erases any specific mention of 'Federal interest' computers. Instead, it defines illegal activity only on computers 'used in interstate commerce or communications.'...Scott Charney, unit chief of the Justice Department's computer crime unit....Using laws that don't clearly apply....Can be problematic, he said. For example, making copies of government computer files might not be stealing because the original copy remains in its computer....The new changes to the act define unauthorized and authorized computer users who damage computer systems as committing crimes of equal severity."

Sikorovsky, Elizabeth; "NSC Proposes to Shift Policy-Making Duties," *Federal Computer Week*, Vol. 9, No. 2, Page 1, January 23, 1995.

KEY WORDS: NSC, policy, NSTISSC, FEMA, NIST, Computer Security Act of 1987.

ABSTRACT: "A new high-level committee would set security guidelines for classified and sensitive-but-unclassified information in Federal computer systems, under a proposal being considered by an interagency operating group of the National Security Council (NSC)....Critics of the plan say it will give military and intelligence agencies more influence over Federal computer security....Formed last September as the result of Presidential Decision Directive-29, the U.S. Security Policy Board is now the chief mechanism for proposing legislative initiatives and executive orders relating to U.S. security....New committee, called the Information Systems Security Committee (ISSC)....Some of this nation's most significant vulnerabilities lie within the sensitive-but-unclassified networks that perform the basic functions that we all take for granted....Would reverse current information policy. Under the Computer Security Act of 1987, the National Institute of Standards and Technology, with technical support from NSA, has responsibility for creating policy guidelines for sensitive-but-unclassified information....Policy making for classified information is handled by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISSC includes representatives from the National Security Council, the Office of management and Budget, the Joint Chiefs of Staff, the Defense Intelligence Agency, the CIA, the General Services Administration, the Federal Emergency Management Administration and the FBI as well as the departments of Defense, State, Treasury, Justice, Commerce, Transportation and Energy and the Army, Navy, Air Force and Marine Corps. Jointly chaired by DoD and OMB, the new committee would consist of voting representatives from civilian agencies that NIST represents under the Computer Security Act, NIST, representatives from all the agencies currently represented on NSTISSC and 'other appropriate agencies,' such as the Defense Information Systems Agency. ISSC, on the other hand, would be responsible for both types of information. Because ISSC would report to NSC directly....Privacy advocates have criticized the proposal....'The prospect of NSA and other Defense intelligence agencies assuming such an expanded role is quite disturbing. This shows that the only chance for any genuine dialogue for public accountability lies with the Congress,' said Joan Winston, project director for the Office of Technology Assessment report 'Information Security and Privacy in Network Environments.' "

Sikorovsky, Elizabeth; "OMB A-130 pushes for personal accountability," *Federal Computer Week*, Page 1, March 27, 1995.

KEYWORDS: Policy, OMB

ABSTRACT: "Changes to the Office of Management Budget's Circular A-130 could radically shift information security responsibilities by making individuals more accountable than ever for securing their own PCs. ..... In its first update to A-130's security policy in 10 years, OMB has moved away from its earlier approach of setting technical requirements for centralized, glass house environments. Instead, OMB is directing agencies to adopt minimum-security management controls and is requiring that all end users be trained in security for their assigned systems. ..... The proposal, called Appendix III to OMB Circular A-130, would require agencies to establish written rules of behavior tailored to users of specific systems. The rules would provide guidelines for working at home, dial-in access, connecting to the Internet, using copyrighted software, system privileges, individual accountability and other situations. The proposal would also require that users receive 'specialized awareness and training focused on their responsibilities' ..... To ensure that training is taking place, OMB would require agencies to assign an individual to oversee each sensitive system. ..... OMB has the authority to deny funding to agency systems deemed insecure, he said. Dorothea deZaffra, information systems security officer for the Public Health Service and past chairwoman of the Federal Information Systems Security Educators Association, said training costs would overwhelm agencies."

Sikorovsky, Elizabeth; "McNulty plans to retire, start infosec practice," *Federal Computer News*, Page 3, March 27, 1995.

KEYWORDS: NIST, McNulty

ABSTRACT: "Lynn McNulty, associate director for computer security at the National Institute of Standards and Technology, has announced he will retire April 28 after six years at NIST. He plans to start a consulting practice specializing in information security issues. McNulty will also step down from his posts as executive secretary of the Computer Systems Security and Advisory Board and co-chairman of the Federal Agency Computer Security Program Managers' Forum. As policy liaison between NIST and other organizations, McNulty's main responsibility has been to enforce the Computer Security Act. The act gives NIST sole authority to develop guidelines and standards for non-classified-but-sensitive information. ..... No successor has been named, although Ed Rohrbach, part of McNulty's staff, will take his place in the interim."

Sikorovsky, Elizabeth, "U.S. to help build Global Info Infrastructure," *Federal Computer Week,* Page 8, March 6, 1995.

KEYWORDS: GII, emergency response, G7

ABSTRACT: "Government agencies will help build 11 Global Information Infrastructure applications as part of an international collaboration announced at the recent Conference in Brussels. ... G7 GII Projects Include: .... A global management network to enhance emergency response management."

Sikorovsky, Elizabeth, "Internet break-ins compromise NASA data," *Federal Computer Week*, Page 4, December 19, 1994.

KEYWORDS: Internet, NASA, hackers, Europe

ABSTRACT: "A steady increase in Internet hacker attacks is putting NASA research programs and missions at greater-than-ever risk, agency officials have confirmed. The increases in attacks 'are not statistical anomalies,' said Rick Carr, NASA's information technology security program manager. 'They are the beginning of a trend of more sophisticated, harder-to-detect attacks,' ..... NASIRC, formed in January 1993 and located at Goddard Space Flight Center, is NASA's central reporting, assistance and coordination point for handling computer information security problems. NASIRC aids the NASA centers, which are individually responsible for their own security management. ..... Car said that break-in attempts at some NASA centers have increased to around 1,000 a month -- nearly fourfold over the last two to three years. Since November of last year, NASA has documented six 'high impact' attacks that have compromised sensitive or classified information. Losses were put at more than $250,000 per incident. ..... 'There's no downsizing in the Internet, but there's a lot of downsizing at NASA,' said Frank Martin, deputy computer security manager for Johnson Space Center's Information Systems Directorate. ..... As the Internet continues its explosive growth, so does the vulnerability of NASA computers, with more than 100,000 NASA-affiliated systems now thought to be exposed to the Internet. ..... Intrusions have resulted in theft and damage of research data and the use of NASA computers and storage devices. ..... Carr said $30,000 bounties have been offered in Europe to challenge hackers to break into NASA systems. ..... Solutions to growing hacker threats include employing more secure software, educating users and sharing information among systems managers. Automated tools that can recognize if, where and when a network is being attacked are invaluable, Carr said, though much of this software has not hit the commercial market."

Sikorovsky, Elizabeth; "Guidelines expected to step up security efforts," *Federal Computer Week*, Page 6, February 20, 1995.

KEYWORDS: COMPUSEC, National Research Council, Generally-Accepted System Security Principles (GSSP), NIST

ABSTRACT: "An international industry/government group in April is expected to propose a first-ever set of core guiding principles for boosting computer system security. The guidelines would also be used to establish more formal standards for how security can be measured within an organization. 'What we're envisioning is a whole structure for professionalizing computer security...something you could audit against,' explained Will Ozier, chairman of the Generally-Accepted System Security Principles (GSSP) Committee. The guidelines would become an authoritative point of reference that would be accepted internationally, he said. ..... The GSSP Committee was formed following recommendations of a ground-breaking 1990 National Research Council report titled 'Computers at Risk.' .....

- Accountability.
- Relevant and easily accessible information on how a system has been secured.
- A code of ethics related to security.
- Security procedures that take into account the needs of all relevant and involved parties.
- Responsible risk assessment.
- Coordinated approaches to implementing security.
- Timeliness in prevention and response.
- Regular reassessment.
- Sensitivity to the rights of users.
- Competent security personnel.

..... The guidelines will be recommended but not required for U.S. government agencies, NIST said. ..... NIST plans to offer some of its own agency documents and studies for possible integration into the GSSP guidelines, including NIST's Common Criteria Guidelines and a security handbook under development called 'An Introduction to Computer Security: A NIST Handbook."

Sikorovsky, Elizabeth, "ARPA, NSA combine research forces," *Federal Computer Week*, Volume 9, Number 8, Page 8, April 10, 1995.

KEYWORDS: ARPA, NSA, DISA, INFOSEC

ABSTRACT: "The Advanced Research Projects Agency and the National Security Agency are combining their efforts on information security research. A new Information Systems Security Research Joint Technical Office will help link the two agencies research for the Defense Department, including the area of electronic commerce. ..... In the areas of secure computing systems, secure networking and assurance technology, 'NSA is focused on satisfying the needs of the next two to five years, whereas ARPA is looking at the next decade. The coordination is to make sure NSA's short-term strategy and ARPA's long-term strategy are lined up,' ..... ARPA performs its research in unclassified environments, ... NSA research takes place in a classified environment. ..... The two agencies will begin to jointly fund research in information security, the DoD spokesperson said. ..... It will also 'bring together private-sector leaders in information systems security research to advise...and build consensus for the resulting programs.' .....

- Reviewing and coordinating all Information System Security Research programs at ARPA and NSA 'to ensure there is no duplication.'
- Maintaining a channel for exchanging technical expertise.
- Providing long-range strategic planing for information systems security research.
- Working with DISA, other Defense organizations and academic and industrial organizations to incorporate new information systems security research into prototype systems and test-bed projects."

Sikorovsky, Elizabeth, "Livermore unleashes 'angel' against threat of SATAN," *Federal Computer Week*, Volume 9, Number 8, Page 38, April 10, 1995.

KEYWORDS: National Laboratories, Livermore, SATAN, CIAC, Courtney

ABSTRACT: "Nicknamed the 'angel' program, a new software tool developed at Lawrence Livermore National Laboratory will help computer operators protect themselves against SATAN, a just-released computer program sure to be used by hackers worldwide. ..... To help combat SATAN, Livermore computer security specialist Marvin Christensen developed the 'angel' software -- officially called

Courtney, after his daughter -- to alert a system operator when a SATAN attack is being launched on a system. ..... Courtney does not protect a system against hacking; it only acts as a tripwire to announce when SATAN is working on a system. 'It gives you a heads-up,' Feingold said. ..... Courtney is available free on the Energy Department's Computer Incident Advisory Committee (CIAC) Internet site: 'http://ciac.llnl.gov/ciac.Tools UnixNetMon.html#Courtney.' SATAN is available on the ftp site 'ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z."

Sikorovsky, Elizabeth, "Energy Department to sell security services," *Federal Computer Week*, Volume 9, Number 9, Page 28, April 24, 1995.

KEY WORDS: DoE, CIAC, security services, OMB, A-130, CERT

ABSTRACT: "Envisioning a gold mine in a proposed government computer security requirement, the Energy Department is offering Internet security services to civilian agencies on a fee-for-service basis. DoE's Computer Incident Advisory Capability (CIAC), which previously responded to intrusions or viruses in DoE systems only, is expanding its offerings in response to the Office of Management and Budget's proposed Appendix III to its Circular A-130. ..... The proposed appendix also calls on agencies to provide a plan for dealing with computer security emergencies. ..... The proposed appendix 'does not specifically state that [agencies] would have to make their own' security response team, said Phil Siebert, a computer security specialist under DoE's deputy assistant secretary for information management. 'I would imagine that the most cost-effective way to go about that would be through some other service,' Siebert said. Housed at DoE's Lawrence Livermore National Laboratory, CIAC expects to increase its staff depending on how interested civilian agencies are in the service, Siebert said. CIAC's expanded services come at a time when other computer security response teams are inundated with work. ..... the Computer Emergency Response Team at Carnegie Mellon University 'last year had to send out a message to say, 'Unless you have a big problem, don't call us. We're overwhelmed.' "

Silver, Judith, "Routine workouts keep VA security tight," *Government Computer News*, Page 71, August 8, 1994.

KEYWORDS: VA, VHA, COMPUSEC, electronic signatures

ABSTRACT: "Peter J. Groen, director of the Veterans Health Administration's National Center for Information Security in Martinsburg, Va., likes to think that his agency takes such a proactive, multifaceted approach. NCIS establishes national policy and guidelines for VHA, and provides local facilities with training and security awareness materials. Groen oversees the information security program for all VHA computer systems and networks, a universe that

includes 172 medical centers, 350 outpatient clinics and 130 nursing homes nationwide. Eight full-time analysts work on security at the National Center for Information Security. 'We test for weaknesses in order to strengthen the package,' Groen said. 'We put ourselves in the position of someone trying to get access and try a variety of techniques to prevent wrongdoing,' he explained. .....
To secure its enterprise network, VHA runs a specially developed in-house security software called VA Kernel. Users call up specific modules of the VA Kernel depending on what feature they need. VA Kernel is written in M, or what used to be known as Mumps, a language long popular at VA for writing medial applications. VA's M apps run on Digital Equipment Corp. VAX minicomputers with the VMS operating system, or on Unix or DOS microcomputers, depending on the size of the facility. The modules cover a wide range of security issues:

- Access controls who has access to which data. A password identifies users, where they work and what data they can access. Different security levels are assigned to each application, all files within each application and all fields within a file. Employees must periodically change their passwords.
- Audit control tracks who signs on when and to which files. Data on every person and device is logged into a file and reports are made available to information security officers, on-site at every center. The system triggers a mail message or alarm is an unauthorized person looks at sensitive patient files.
- The user management module assigns different levels of control and access. It tracks users throughout their VHA careers, maintaining data for 10 years in the event VHA needs to reconstruct an incident.
- Device handler manages all the peripherals connected to the software. as a device is added to the network, the system records its location and its use. For example, if a device designated not to be used between 8 p.m. and 8 a.m. is accessed during these hours, the system locks up, sometimes without the intruder's awareness. ...

VHA employs a variety of other security measures. Incremental backup is done every ten seconds. Transactions are copied to a duplicate -- and removable -- disk array, which is subsequently locked away. Groen said VHA has been fairly secure against viruses. systems managers installed 20,000 copies of F-Prot Professional from Command Software Systems Inc., Jupiter, Fla, to scan for multiple viruses. But the VHA is still grappling with several security issues. For example, electronic signatures have long been used in the areas of payroll, procurement, medical prescriptions and lab tests. 'We've had our own approach to electronic signatures, but now will start to fall in line with the standard,' said Groen. 'We've had years of experience meeting whatever draft standards existed at the time.' Until now, VHA has dealt mainly with internal security issues, but as e-mail and Internet traffic increase, new opportunities for security breaches exist. VHA recently expanded the capability of its Internet gateway at its Washington Information Support Center. The solution: Build a firewall of hardware, software and procedures to protect the internal network. VA uses DEC's Screen External Access Link (SEAL), consisting of filtering routers and application gateways. It functions by screening out data with source addresses that have not been preapproved by the system administrator. The software defines the parameters of what will be let in. 'It was easier to exercise control when security was handled on a mainframe computer system connected to dumb terminals,' Groen said, but 'everyone is going through the same problems in both the private and public sector, not just in health care.' VHA is also trying to anticipate the future in regard to encryption software."

Skinner, Liz, "Global Positioning Systems' Place on Infobahn," *Washington Technology*, Vol. 9, No. 18, Page 14, December 22, 1994, TechNews, Inc.

KEYWORDS: GPS, paging, FCC

ABSTRACT: "24-satellite constellation completed last year. Cost $12B. Foundation for navigation, surveying, boating, aviation. New applications being explored for paging (for shipping and freight companies, stranded motorists, etc.). Precise timing required for scheduling transmission of messages. Trimble Navigation, Sunnyvale, CA, and Magellan Corporation, San Dimas, CA, teaming to help paging companies. Magellan being acquired by Orbital Sciences Corporation, Dulles, VA. Recent FCC ruling on channel sharing for private carrier paging operations demands efficiency."

Smith, Emily T.; "Will Lasers Blast Through the Data Bottleneck?," *BusinessWeek*, Page 91, February 20, 1995, A McGraw-Hill Publication.

KEYWORDS: laser, satellite, mobile phone

ABSTRACT: "In the future, though, if Thermo Trax has its way, lasers may help satellites transmit more data. Laser light can carry up to 1 billion bits of information per second....Thermo Trax's 'pods,' which would be added to satellites to receive and send the laser beams, weigh just 30 pounds and cost under $100,000. Lasers are also more secure. Radio waves can spread out up to a mile when transmitted, which makes it easier for data to scatter to unintended receivers. but the thermo Trax system can be focused into a beam as little as 1.5 centimeters wide."

Smith, James M.; "Logic flaw is the culprit in computer 'mugging'," *Government Computer News*, Page 12, November 7, 1994.

KEYWORDS: Medicaid, EC/EDI, Electronic fund transfer

ABSTRACT: "A software glitch has been fingered in the case of a $70 million 'purse snatching.' After disbursing the money in overpayments for health plans they administer, the Health Care Financing Administration discovered the glitch in software that pulls data from three databases. ..... Bob Goldrick, director of

HCFA's Office of Enrollment Systems, said the overpayments were generated when software for the Group Health Plan System automatically retrieved one status update from the Medicare Enrollment System on whether certain individuals had Medicaid, but not another on those who had lost their Medicaid privileges, he said. About 100 health care organizations received overpayments, the largest about $19 million, according to HCFA records."

Sprehe, J. Timothy, "Federal Information: Who Owns It?," *Federal Computer Week*, Vol. 9, No. 3, Page 1, February 6, 1995.

KEYWORDS: Information Industry Association, NII, government databases, Freedom of Information

ABSTRACT: "Information Industry Association...are the so-called information providers -- companies such as Dun & Bradstreet, McGraw-Hill and America Online -- that sell information services rather than information technology services....'Principles for Federal Dissemination of public Information' can be seen as the information industry's own circular A-130....principle of diversity...Federal agencies should disseminate government information, but non-Federal parties should do so as well....The temptation government must avoid is behaving like a purely self-interested monopolist, restricting the channels of access to protect the government's own market for the information. IIA contends that if an agency offers for sale information services based on its databases, the agency should also permit the public to buy the underlying databases themselves....Industry wants to do business by adding more value and reselling the information without any strings attached....You can get a copy of the 'Principles for Federal Dissemination of Public Information' from the Information Industry Association, 555 New Jersey Ave. N.W., Suite 800, Washington, D.C. 2000, (202) 639-8262....Sprehe is president of Sprehe Information Management Associates, Washington, D.C. He can be reached via the Internet at jtsprehe@access.digex.net."

Sprehe, Timothy J., "Public-interest groups want too much too soon," *Federal Computer Week,* Page 15, November 7, 1994.

KEYWORDS: OMB, NIST, Government Information Locator System

ABSTRACT: "The Office of Management and Budget is all set for the official launch of the Government Information Locator System (GILS), but public-interest groups are trying to delay or abort the countdown. ..... OMB intends to decree that all executive-branch agencies must establish publicly available inventories of their print and electronic publications in a common format to be promulgated in a Federal Information processing Standard that the National Institute of Standards and Technology will issue. The FIPS that comes out of NIST will define a "GILS core," a kind of bare minimum of data elements to which each agency must adhere. OMB's directive for GILS envisions a system in which each agency produces a standardized database containing metadata -- that is, information about information. The database records will be bibliographic in nature. They will not contain the actual agency publications but will describe those publications and how to acquire them. Some public-interest research groups, led by OMB Watch, want much more. They want OMB to insist that GILS be redesigned so that on-line users of GILS could click on a bibliographic entry and be transferred directly to the full text of the publication itself.

Stahlman, Mark, "The Encryption Enigma," *Information Week*, Issue 523, Page 104, April 24, 1995.

KEYWORDS: Export, NATO, France, encryption

ABSTRACT: "Current U.S. export restrictions on 'strong' encryption, and the related key-escrow proposals from the Clinton administration, are important enough for every business that they are now front-page news. Network security -- particularly on the Internet -- is potentially the biggest technical limit to expanded net-based business. ..... The dilemma with France is this: NATO is in trouble; the U.S. relationship with France is *really* in trouble. If the United States were unilaterally to release restrictions on 'strong' crypto it could create an international incident with a high probability of being used by France as the reason it would pull out of NATO. ..... In France, all decent encryption technology is simply illegal. The only crypto-technology permitted is on an official list that is widely known to contain only systems that French intelligence services can easily break. ..... A U.S. decision to open the U.S. borders to the free flow of this technology -- via no less than an Act of Congress in this case -- would be a severe slap at France's sovereignty. ..... Mike Nelson, Vice President Al Gore's chief techno-staffer, has said the U.S. crypto-export prohibition will not go away anytime soon and is a direct result of requests from unnamed allies."

Sussman, Vic, "Lost in Kafka territory," *U.S. News & World Report*," Page 32, April 3, 1995.

KEYWORDS: Pretty Good Privacy, encryption, export, NIST, EFF, DES

ABSTRACT: "If anyone on Earth can claim to be a cyberspace celebrity, it is Philip Zimmermann, a soft-spoken data security consultant from Boulder, Colo. ..... This week, the Electronic Frontier Foundation, a cyberspace civil liberties organization, will give Zimmermann a prestigious Pioneer Award, for helping protect citizens' privacy by creating a powerful encryption program called 'Pretty Good Privacy'.(PGP) and making it available for free. ..... But law enforcement and intelligence officials have a different view of Zimmermann's achievement. He is being investigated for possible violation of Federal arms-export laws because his 'cryptography for the masses' has slipped out of America. ..... a grand jury in San Jose, Calif., has been gathering evidence since 1993, pondering whether to indict Zimmermann for violating a Federal weapons-export law -- a charge that carries a presumptive three-to-five-year sentence and a maximum $1 million fine. ..... a grand jury indictment must be authorized by the Justice Department in Washington. Zimmermann's woes raise big questions. Can machine-age law be applied fairly to rapidly developing technology? Is putting software on a computer the same as exporting it? ..... Oddest of all, it is perfectly legal for a foreign bad guy to buy books containing encryption codes and type them into a computer. **Oops!** If Zimmermann is indicated as an alleged arms merchant because his cryptography ended up in foreign hands, then somebody in the U.S. government probably should be prosecuted, too. In 1993, the National Institute of Standards of Technology (NIST) inadvertently placed DES, a strong encryption program, on one of its Internet-linked computers. Word spread quickly in cyberspace, and a *U.S. News* reporter easily found a file copy on a computer in Finland. A NIST spokesman sheepishly admitted that the accidental crypto 'export' was a mistaken attempt to help U.S. computer users strengthen their security.

Sussman, Vic, "Policing Cyberspace," *U.S. News and World Report*, Vol. 118, No. 3, Page 55, January 23, 1995.

KEY WORDS: crime, law enforcement, Internet

ABSTRACT: "Kevin Manson...Federal Law Enforcement Training Center...'Crime involving high technology is going to go off the boards,' predicts FBI Special Agent William Tafoya....Advantages of...Ability to link millions of computer and modem owners...technological breakthroughs, such as digital encoding...Wide-open culture...The crimes that worry authorities the most:
•**White-collar crime.** Virtually every white-collar crime has a computer or telecommunications link....Kevin Mitnick, currently America's most wanted computer criminal....
•**Theft.** Salami slicing...Pilfering industrial secrets. Last November, someone infiltrated Internet linked computers owned by General Electric and stole research materials and passwords....
•**Stolen Services....**
•**Smuggling.** Launder....
•**Terrorism....**Cracker -- Cyberspeak for a malevolent hacker -- might penetrate FedWire....Cracker testing....
•**Child Pornography.** FLETC's Financial Fraud Institute conducts some 14 programs, regularly updated to keep pace with wrinkles in crime....But legal access to data is only part of the problem. Another difficulty is unauthorized peeking into personal records....Malicious tipsters can poison a person's record

with innuendo....The United States has a law barring release of video rental records but no strong laws against scanning personal medical data....The new Congress will soon begin deliberations over proposals that would offer privacy protections for Americans' medical, credit and telecommunications data....There is widespread agreement across the Internet and among entrepreneurs hoping to do business in cyberspace that cryptography is necessary for privacy in a networked universe....Businesses....Electronic mail....E-mail....Bruce Schneier....'E-mail Security: How to Keep Your Electronic Messages Private.'...Jim Kallstrom....We merely think that criminals, terrorists, child abductors, perverts and bombers should not have an environment free from law enforcement or a search warrant....The FBI won a round last year when Congress passed the Digital Telephony Act, which requires future telecommunications systems to be accessible to wiretaps....Electronic Privacy Information Center's Marc Rotenberg, who calls Clipper part of the "Information Snooperhighway....Law enforcers are also deeply worried about anonymous re-mailers....Anonymous re-mailers outside the reach of American authorities are being used by electronic vandals to bedevil their victims with threatening messages or 'mail bombs' composed of thousands of gibberish messages....The simple truth, though, is that no legislative act can stop the spread of cryptography....Cryptography will become even more popular once cybersurfers discover digital cash....Robert Corn-Revere, a former Federal Communications Commission official who now practices First Amendment law. He argues that the day is passing when government can justify licensing and regulating media....People create their own communities in cyberspace, based on affinity rather than geography....John Perry Barlow....Suggested in a widely read *Wired* magazine article that traditional notions of copyright were dead in cyberspace....Ken Wasch, executive director of the Software Publishers Association, says pirated software costs the industry $9 billion a year."

"Tech Thrusts," *Aerospace Daily*, Vol. 172, No. 6, Page 41, October 11, 1994.

KEY WORDS: Air Force, Senate Armed Services Committee

ABSTRACT: "Gen. Ronald R. Fogleman, in line to be the next Air Force chief of staff, says that during his tenure the major technology thrusts will be optimizing information management systems to serve as force multipliers....He sees 'few quantum leaps' in technology related to hardware and munitions."

"Texas Department of Transportation Wins CSI'S Computer Security Program of the Year Award," *Pr Newswire (PRNW)*, December 2, 1994.

KEY WORDS: Computer Security Institute, Computer Security

ABSTRACT: "William Tompkins, INFOSEC Mgr, Texas Department of Transportation, won CSI's 1994 Security Program of the Year

Award....Computer Security Institute is the oldest international membership organization specifically assisting the information security professional. CSI sponsors two annual security conferences, holds regional training classes and offers a membership package that includes monthly newsletter, journal, buyers guide, hotline, training discounts and more. CSI can assist with background research in the computer and information security areas."

"Think Before You Leave the Country with Your Cellular Phone," *Export Control News*, Vol. 8, No. 10, Export Control News.

KEY WORDS: cellular phone, export controls

ABSTRACT: "Toting your cellular phone on overseas trips may earn a few violations of U.S. export controls in the process....Cellular phones, like encryption software, create real, and sometimes problematic, export licensing issues. The U.S. export controls applicable to mobile cellular telephones depend on the encryption capability they employ. There are three categories: cellular phones that do not employ encryption, cellular phones that encrypt an entire transmission, and cellular phones that employ encryption for limited purposes such as password encryption....The Commerce Control List (CCL) in the Export Administration Regulations (EAR)." "U.S. Munitions List (Category XIII) in the International Traffic in Arms Regulations (ITAR)."

Thorat, Dana, "Network Help Desk," *Network World*, Vol. 11, No. 47, Pages 2, 54, November 21, 1994.

KEY WORDS: mainframe, LAN security

ABSTRACT: "John Abolins, an administrative analyst for the New Jersey Department of Environmental Protection in Trenton, replies." "Stephen Cobb, a technology analyst at the National Computer Security Association adds: The National Institute of Standards and Technology (NIST), which is a part of the Department of Commerce, cosponsors the annual National Computer Security Conference with the National Computer Security Center, which is a part of the National Security Agency (NSA). Cosponsored with the Air Force Information Warfare Center, NIST has also recently released a CD-ROM about security, which is based on information from the Forum of Incident Response and Security Teams and put out by the Security Tools and Techniques Resource Library. For more information, contact NIST's Security Division by telephone at (301) 975-2934 or via their bulletin board at (301) 948-5717 (using up to 28.8Kbit/sec, N81 and VT100 modem settings)....For more information about government agency security studies, contact the NSA at (301) 688-6524."

Varon, Elana, "On guard with IRS' privacy watchdog," *Federal Computer Week*, Page 24, November 14, 1994.

KEYWORDS: IRS, privacy, National Research Council

ABSTRACT: "Robert N. Veeder, the Internal Revenue Service's first-ever privacy advocate, has spent most of his career mediating between government demands for personal data and an individual's desire to protect his privacy. ..... So although he was hired to develop privacy policies for the IRS to complement its Tax Systems Modernization (TSM) program, Veeder intends his program to become a model for protecting individual privacy that other agencies can also use. ..... When the official in charge of privacy policy at OMB, Leslie A.L. Borden (who Veeder later married), moved to a new job, Veeder took over and stayed until the IRS hired him in June. Borden no longer works for the government. Veeder's IRS job was first suggested by the National Research Council in its comprehensive review of TSM. The council wanted the IRS to highlight privacy issues as it revamped its operations to give employees access to a wider range of personnel data. Veeder's office has two functions: develop and analyze legislation concerning taxpayer privacy and develop privacy guidelines for IRS employees. Recently his office completed a privacy training film that each of the IRS' 110,000 employees was expected to see by the end of September. His staff is also developing a manual to help employees carry out their legal and ethical responsibilities. Meanwhile, Veeder said, he wants the IRS to incorporate privacy protection into its systems design."

"The Weird Stuff - Pentagon Policy," *Flight International*, Page 35, August 3, 1994.

KEYWORDS: policy, Gulf War, C2W, Deception, Operational Security, United Kingdom

ABSTRACT: "Pentagon Memorandum of Policy No. 30, 1993 [has been] signed off by the UK Chief of Staff as being a recognised aspect of future military policy....Speaking at the Tele Krig electronic-warfare symposium in Stockholm, Sweden in June, "Col David Tanksley, then chief of the Pentagon's C2W and EW branch, said that the USA Rival implemented the concept during the planning phase for Operation Desert Storm....The planning phase....Gulf War Weapons....*Offensive* goals of C2W (slowing the enemy's pace of operations, disrupting planning and decision-making capacity and degrading the ability to implement decisions)....EW aircraft....EA-6B and EF-111A....Psychological warfare....Air National Guard's EC-130 Volant Solo radio, and television-broadcast aircraft. Precision strike tasks employed aircraft as varied as the Lockheed F-117A and the F-16, General Dynamics F-111, the McDonnell Douglas F-15 and F-18, the Northrop Grumman A-6 and the U.S. Army's McDonnel Douglas AH-64 attack....Texas Instruments (TI) AGM-88 high-speed anti-radiation missile (HARM) and cruise missiles....Acquisition of the intelligence necessary....Included the Lockheed U-2R, Boeing RC-135 Rivet Joint and U.S. Navy Lockheed EP-3 Aries II....Tanksley....Paralysing the leadership. Of U.S. air operations flown during the campaign, 10% were dedicated to engaging C2 targets, 25% were against air defence or tactical targets....A deception campaign....A seaborne invasion of Kuwait, and *own-force* security measures, such as flying airlift operations below the Iraqi radar horizon and *absolute* communications security....Cdr Frank Folly, a member of USA's Joint EW Center at San Antonio, Texas....The EW component [consists of] electronic attack, electronic protection and electronic support....Recognises that EW operations only offer short-term effectiveness, while also posing a risk to the friendly use of the electro-magnetic spectrum and the danger of fratricide....Targeting decisions should also be weighed against whether the survival of a particular node can be exploited to 'advantage' by another element of C^2W doctrine....Operational-security tactics are intended to 'hide the truth' from the enemy....Tanksley cited the threatened use of the devastatingly effective BLU-82 fuel-air munition....Of 32 tri-service systems quoted by Folly as supporting the concept of C^2W....Potential targets for C^2W, Folly picks out the cellular telephone, satellite communications and the global-positioning system....1W GPS jammer capable of blocking civil reception within a 22km (12nm) radius. A 64W output increases the jamming radius to 175km....The Pentagon has developed a C^2W/Information Warfare course, with three training centres already teaching the doctrine as a basic element of the syllabus."

Wilder, Clinton, "A Matter Of Standards," *Information Week*, Page 14, March 13, 1995.

KEYWORDS: Internet, security, WWW, encryption, RSA

ABSTRACT: "A standards battle is brewing over Internet transaction-security protocols. ..... As server software that enables secure transactions begins to hit the market, two different security standards are emerging. Most vendors of the World Wide Web server and browser software are backing the Secure HTTP standard, which encrypts and secures transactions initiated by the Web's Hypertext Transfer Protocol (HTTP). But Netscape Communications Corp., whose Netscape Navigator grabbed the early market lead among Web browsers, uses an internally developed Secure Sockets Layer (SSL) encryption method for Web transactions. ..... Although new server software using secure HTTP will enter the market as early as March 6, until now, Netsite has been the only server software available for Web transactions. ..... Spry, Spyglass, Open Market, the CommerceNet consortium, and other Secure HTTP supporters are accusing Netscape of trying to bulldoze the market with SSL. ..... Open Market in Cambridge, Mass., will roll out its transaction server products, Open Market WebServer and Secure WebServer on March 6. ..... SSL simply encrypts the data in a given file, such as a customer information form with a credit-card number, and decrypts it at the other end of the transaction. Secure HTTP is a more comprehensive security package that includes authentication of the client's identity by the server through digital signature verification and other features. ..... Secure HTTP has moved much further than SSL down the official paths of the two most influential Internet standards bodies, the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). ..... Jeff Treuhaft, a project manager at Netscape ..... Treuhaft claims that Web users need security for transmission methods other than HTTP (such as FTP and Telnet), which SSL provides. 'Secure HTTP doesn't have any value whatsoever outside of HTTP transactions,' he says. ..... both standards are based on core algorithms from RSA Data Security Inc. in Redwood City, Calif., that scenario ..... ."

Wilder, Clinton, "How Safe is the Internet?," *Information Week*, Page 13, December 12, 1994.

KEYWORDS: Internet, firewalls, GE, RSA

ABSTRACT: "Sometime during the week of Nov. 21, unidentified computer hackers bore through GE's Internet security "firewalls" and accessed GE systems that contained proprietary information. ..... 'You have to evaluate what you will do over the Internet and what risks you're willing to take,' says Jerrold Grochow, VP and chief technical officer at American Management Systems Inc. (AMS) in Fairfax, Va., ... Tyson Foods Inc. in Springdale, Ark., says it won't bring up a Web server for at least a year, or until it has developed a firewall that is 'very secure,' says Steve Hankins, VP of information systems. ..... Just one day after news of its hacker break-in came to light, GE announced that four of its business units joined CommerceNet, the Menlo Park, Calif., consortium of companies seeking to promote business transactions on the Net. ..... Another potential risk of business in cyberspace stems from the culture clash between corporate America and Internet purists who fear the Net's free-spirited commune will be torn up and replaced by a giant online shopping mall. ..... The vast majority of Internet break-ins go unreported. ..... Internet security falls into two basic categories: firewalls that protect internal information, and encryption schemes that encode business transactions, particularly credit-card authorization and debiting. ..... Microsoft Corp. and Visa International agreeing to develop a system based on technology from RSA Data Security. ..... products for secure Internet ..... including Enhanced Mosaic 2.0 from Spyglass Inc. in Naperville, Ill. ..... Matthew Howard, security product manager at router maker Cisco Systems Inc. in Menlo Park, Calif."

Wilder, Clinton and Levitt, Jason, "Cure or Curse?" *Information Week*, Page 14, April 3, 1995.

KEYWORDS: SATAN, Internet, network security

ABSTRACT: "SATAN: Is it a powerful, easy-to-use security tool, or your worst security nightmare? It may be both, and it will be available free to anyone who wants to grab it off the Internet as of April 5. ..... acronym for Security Administrator Tool for Analyzing Networks ..... Satan gets into a site the same way an intruder would, from a host that is not part of the site's local area network. ..... By running this one application, an administrator could learn of myriad security holes and have an opportunity to repair them. ..... And the decision by the Satan developers to offer this product for free via the Internet is frightening many administrators and information technology executives. ..... The program's designers say that the software does not damage systems that it probes, but merely checks to see if security holes exist and reports back its findings. But even if running Satan cannot damage a system, a skilled programmer could modify Satan to be intrusive, as the product will be distributed with complete source code. ..... Satan co-developer Dan Farmer ..... acknowledges the potential for nefarious applications, but insists that a tool that provides data on the vulnerability of a network to administrators is valuable and positive. ..... A recent *InformationWeek* survey of 100 large user sites showed that 71% considered network security one of their highest priorities. And of those users, 61% said they were using no automated security applications at all. ..... 'One of its insidious aspects is the very user-friendly Mosaic interface,' says Donn Parker, of SRI International, a research firm in Menlo Park, Calif. ..... 'Any self-respecting hacker's tool kit already has all the tools that Satan has, without the nice graphical front end,' says Marcus Ranum, an engineering manager at Internet firewall developer Trusted Information Systems Inc. in Glenwood, Md."

Wilder, Clinton and Levitt, Jason, "Not The Devil Incarnate," *Information Week*, Page 15, April 3, 1995.

KEYWORDS: Satan, Internet, network security

ABSTRACT: "..... contrary to some media reports, there are fixes available for all the vulnerabilities that Satan detects, although some of those may involve painful upgrades of operating-system software or even the reorganization of an entire local are network to include a firewall. ..... it is the familiarity and accessibility of the browser interface that makes Satan especially dangerous, ... The entire Satan user interface is implemented using Hyper Text markup Language (HTML) pages and makes good use of HTML forms for filling in information and offering options via push buttons. ..... When the program finds a chink in a system, it describes the vulnerability, and sometimes explains how an intruder would use that weak link to attack. It also details how best to patch the chink to ensure the system's safety. Satan also enables administrators to devise their own security probes. All one needs to do to add a probe to Satan is create an executable that checks for the problem. ..... While the first version of Satan won't damage or actively 'break in' to any sites that it probes, the documentation for Satan says a 'break-in' scanning level, called 'all out,' will be implemented in a future release. ..... At the all-out level, Satan might steal an

/etc/passwd file, rhosts file, or other, normally privileged, operating system software, ... At the core of the Satan program is the Inference Engine module, which consists of five rule bases. The most important rule base allows Satan to deduce potential security problems based on known 'facts' about security problems. For example, one rule says that if a system is running a version of Sendmail earlier than version 8.6.10, then it is probably vulnerable to outside attack. ..... Another module runs the series of programs that probe systems and collect data. ..... The Target Acquisition module takes a list of target hosts, along with the search constraints, and generates the list of security probes that are fed to the Data Acquisition module. ..... Satan's 'intelligence' comes from the way it explores the avenues of trust associated with a target host. Satan can discover hosts that are associated with the target host via Network File System (NFS) mounts or other trusted paths, and then generate new probes to run on those newly discovered hosts. ..... The Report and Analysis module collects all the accumulated data and results for the user to explore. ..... Satan is also easy to get running. All that's needed to compile and run Satan is a C compiler, the freeware language Perl, and a copy of the Mosaic or Netscape Web browser. ..... release of Satan will likely only compile and run cleanly on a few Unix systems (Sun's SunOS and Solaris, and Silicon Graphics' Irix operating system), it will quickly be ported to other Unix systems because administrators will be frantic to test the security at their sites. In a short time, anybody with a 386 or 486 machine running Unix should be able to master Satan in less than an hour. A direct or Serial Line Internet Protocol/Point-To-Point Protocol SLIP/PPP) dial-up connection to the Internet is all that's necessary to start probing other sites with Satan. ..... While Satan takes up only 2 Mbytes of disk space, the Web browser, Perl, and the C compiler can easily chew up another 20 Mbytes, especially if the user has to compile Perl and the browser from source code. Satan needs from 8 Mbytes to 48 Mbytes of RAM, depending on the number of hosts scanned atone time. A user needs to have root authority on a Unix system to run Satan because some of the probes require superuser privileges. For users who just administer Unix systems, this limitation will prevent them from running some of the Satan probes, but, since complete source code is included, they can easily modify Satan to skip those probes."

Wilder, Clinton, "A New Safety Net," *Information Week*, Issue 523, Page 14, April 24, 1995

KEYWORDS: Secure HTTP, RSA, online

ABSTRACT: "IBM, Netscape Communications Corp., and the top three online services companies ..... to unite ..... Secure Hypertext Transfer Protocol (S-HTTP) and Netscape's Secure Sockets Layer (SSL). The vendors have agreed to work with -- and make equity investments in -- a Menlo Park, Calif., Internet developer called Terisa Systems. ..... By June, Terisa will add SSL to its S-HTTP-based Secure-Web Toolkit for World Wide Web software developers, ...

IBM, America Online, Prodigy Services, and CompuServe. ..... Terisa ..... a joint venture between encryption specialist RSA Data Security Inc. and Enterprise Integration Technologies Corp. (EIT), a technology infrastructure provider for the CommerceNet ..... Terisa ..... will then work with the relevant Internet standards committees to get the new hybrid standard approved. ..... some in the industry suggest that the Terisa contingent could actually set back the prospect for reliable secure Internet transactions. ..... competitors stress that Netscape still controls the SSL standard and could potentially add proprietary upgrades and enhancements, even if the current version is an 'open' standard in the public domain. ..... competitors are pushing different approaches. Spyglass Inc. in Naperville, Ill., is one of four members of the Electronic Business Co-Op, a consortium that announced April 10 plans to support secure Internet, credit-card transaction technology without using S-HTTP or SSL. ..... two standards committees, the World Wide Web Consortium (known as W3) and the Internet Engineering Task Force."

Wilder, Clinton, Wagner, Mitch, and Levitt, Jason, "Satan's Surprise," *Information Week*, Issue 523, Page 22, April 24, 1995

KEYWORDS: SATAN, CERT, WWW

ABSTRACT: "..... Fears of widespread hacker break-ins due to Satan (System Administrator Tool for Analyzing Networks) went unrealized, but Net security experts discovered that running the Satan program to analyze the security of a network could, in rare cases, actually help to pen a network to outsiders. ..... Satan, when run with certain World Wide Web browsers (including Netscape and Lynx, but not Mosaic) on a local or wide area network, could expose that Satan host to intrusion from another Web site. Satan co-author Dan Farmer posted a new version (Satan 1.1) on the Internet the next day (http://www.cs.ruu.nl/cert-uu/satan.html). ..... The glitch that CERT warns about can occur if users move immediately from a session running Satan on their network to browsing the Web without first quitting their browser. And even then, that users must immediately go to a site that happens to be using a specific data-capturing application."

Wouters, Jorgen, "We Are What We Speak," *Washington Technology*, Volume 9, Number 20, page 13, January 26, 1995.

KEY WORDS: Buzzwords

ABSTRACT: "The King's English, which has admirably served civilization for centuries, is under assault from the information revolution....Indeed, the inherently complex nature of many new technologies, often defy attempts of companies to describe them in good-old Anglo-Saxon. So they turn to buzzwords, technocratic prefabrications that often succeed only in mystifying the very audience at which they are directed....In Vision Systems Corp. of Tulsa, Okla., boasted in a press release that its product is 'the video conferencing industry's first packet-based, real-time, full-motion, audio and video conferencing solution that was designed exclusively to operate over today's LAN and WAN networking infrastructures, including Ethernet, Token Ring, FDDI, Frame Relay, ATM and ISDN....Dan Spiner, managing director of Progressive Strategies Inc., the New York technology consulting firm....The reality of it is that even 50 percent of the people in the industry do not know what they (buzzwords) mean....The bottom line with buzzwords, Moore said, is timing. They are great for raising money in the early market with venture capitalists and other sources, dangerous in trying to get into the market, very useful for consolidating a position, and tired, old and boring when a company enters the mainstream."

Yang, Catherine, "Flamed with a Lawsuit," *BusinessWeek,* Page 70, February 6, 1995, A McGraw-Hill Publication.

KEY WORDS: Online services, law, free speech, copyright, libel,

ABSTRACT: "A user of Prodigy Services Co....accused...Stratton Oakmont...'This is fraud, fraud, fraud, and criminal!' the user wrote on Oct. 23 on Money Talk....Stratton...filed a $200 million libel suit on Nov. 7 against Prodigy...Stratton argues that Prodigy, which removed the derogatory remarks from its network on Nov. 11, is responsible for all communication on its service....Stratton's case has brought to a head a long-anticipated clash between traditional law and freewheeling computer communications....The basic problem: Existing laws are outdated for today's direct, real-time communications. Aside from libel issues, copyright and pornography laws are also bumping up against the tenets of the virtual world...and...other thorny legal questions, such as intellectual-property and contract disputes, online sexual and racial harassment, and the use of electronic communication to peddle fraudulent sales schemes...court rulings that curtail such free speech could substantially cripple the budding online industry...Unless a solution for governing electronic communication is found soon, many computer experts fear an unparalleled litigation explosion....Kent D. Stuckey, CompuServe's general counsel...is currently fending off a case filed in 1993...by New York-based music publisher Frank Music Corp....Frank Music claims that CompuServe is liable for the infringement even if it didn't know that its subscribers were posting and downloading protected works....CompuServe says it shouldn't be made to pay for such acts on its network unless it knew about them and deliberately ignored them....the Prodigy libel case...is a direct test of how far First Amendment protections will go in cyberspace."

Zurier, Steve, “Security,” *Government Computer News*,” Page 71, August 8, 1994.

KEYWORDS: COMPUSEC, LAN, FIPS, GIPS 185, Clipper, NIST, FIPS 186, Digital Signature Standard, one-time passwords, DoC, NASA, DOS, INS

ABSTRACT: “Computer security was simpler before the era of distributed computing. But the complexity of today’s security implementations doesn’t absolve anyone from building systems that the government and the public can have confidence in. ..... 12 tips for greater LAN security:
1. Add expiration dates to accounts.
2. Limit concurrent user connections.
3. Establish password protection accounts.
4. Enforce periodic password changes.
5. Activate intruder detection/lockout.
6. Ensure that file servers, routers and gateways are maintained in a secure location. 7. Train users on their security responsibilities.
8. Don’t overlook built-in LAN operating system security utilities.
9. Implement virus protection on file servers and workstations.
10. Establish security controls for dial-in/out capabilities.
11. Perform and test backups.
12. Implement an audit strategy to detect unauthorized activity and ensure copyright compliance. ..... The Commerce Department approved FIPS 185 as a voluntary standard for voice communications on Feb. 4. FIPS 185 specifies the controversy-drenched Clipper chip and public-key escrow Skipjack encryption algorithm as a means of securing voice communications. Critics can’t forgive the fact that the government would possess a trapdoor into Clipper-encrypted communications, ostensibly for law enforcement agencies. Issuing the FIPS as a voluntary specification has calmed some critics. NIST approved a digital signature standard on May 17. Known as FIPS 186, DSS will allow users to send authenticated and verifiable electronic messages and documents. The Internal Revenue Service pushed for FIPS 186 because all its efforts to conduct electronic commerce under Tax Systems Modernization depend on the ability to send signatures over networks electronically. DSS uses the Digital Signature Algorithm and NIST’s hashing standard to authenticate and validate an electronic message. DSS also embodies a non-repudiation feature, which means that the sender can’t deny that he sent the message. The DSS is also controversial, because vendors seeking to use DSS face lawsuits from Public Key Partners Inc., which alleges the government infringed on its patented public-key encryption methods. ..... Rick Carr, information technology security program manager at NASA, said that since all the issues surrounding DSS have yet to be fully resolved, and Federal funding is tight, he has shied away from the multimillion-dollar project approach. Carr’s idea is to phase security into the network incrementally, starting with building a secure communications system for NASA’s security officers at each NASA facility. He’ll move next to the agency’s financial systems and finally branch out to NASA’s numerous scientific

and engineering departments. ‘We’re exploring the possibility of issuing some kind of token or smart card that could be used as a badge [as well as] to access a user’s computer. It would have digital signatures and encryption for access control built-in to the card,” Carr said. ..... Kim Clancy, who manages the Automated Information Systems Network for the Bureau of the Public Debt. Clancy uses tokens from Enigma Logic Inc., Concord, Calif., to manage user access to sensitive mainframe data. when a user wants to access the mainframe, he or she logs on to the workstation with a stagnant password, which then quickly issues an eight-character password. The user then types the eight-character password into the token, which resembles a handheld calculator running the same mathematical equations as the mainframe. Finally, the token kicks out a one-time password that’s acceptable to the mainframe. ..... Computer telecommunications security program manager at the Immigration and Naturalization Service, echoed a general consensus that security must be viewed from an enterprisewide perspective. She also underscored the need to educate local area network administrators on risk assessment analysis and general security techniques. ‘We’ve been actively training our LAN administrators throughout the INS on security,’ Keys said. ‘This includes training in risk analysis, contingency planning, preparing security controls, and how to identify threats and vulnerabilities and act accordingly,’ she said. ‘It’s a real eye-opener for them to be educated in the critical role security plays in managing an enterprise network,’ Keys concluded.

Zurier, Steve, “State computer analyst puts visas on line for non-users,” *Government Computer News,* Page 72, August 8, 1994.

KEYWORDS: DOS, COMPUSEC

ABSTRACT: “Philip Katner ..... As a computer analyst for the Consular Systems Division of the Consular Affairs Executive Office ..... Katner does the lion’s share of the development work for the Consular Affairs’ Personal Computer-Machine Readable Visa program, the project that is automating visa processing at 110 of the State Department’s 180 posts worldwide. ..... Katner uses PC/DACS and Site/DACS from Mergent International Inc., Rocky Hill, Conn., to secure PC-MRV data. ..... The PC-MRV modules operate under D2 level security, the highest rating for an MS-DOS product. ..... Another big selling point for PC/DACS is that is offers C2 functionality. Some of these features include:

- Object reuse. The object reuse feature cleans out terminate-and-stay-resident instructions and random access memory when users reboot.
- Discretionary access control. Allows Katner to separate the data from the users.
- Auditing. This feature tracks every event on the microcomputer.
- Encryption. PC/DACS allows for custom encryption. Options include encrypting the file allocation table, specific files or the entire hard drive.”

OTHER REFERENCES

Bell Communications Research, *Generic Requirements for Data Communication Network Security,* Bellcore, New Jersey, January 1, 1994.

Cheswick, William and Steven Bellovin, *Firewalls and Internet Security; Repelling the Wily Hacker,* Addison-Wesley, Massachusetts, 1994.

Communications Law--Compilation of Selected Acts Within the Jurisdiction of the Committee on Commerce, U.S. Government Printing Office, Washington DC, 1995.

Computer Science and Telecommunications Board, National Research Council, *The Changing Nature of Telecommunications/Information Infrastructure,* National Academy Press, Washington DC, 1995.

Computer Science and Telecommunications Board, National Research Council, *Realizing the Information Future; The Internet and Beyond,* National Academy Press, Washington DC, 1994.

Defense Information Systems Agency, *Defense Information Infrastructure Master Plan, Version 2.0,* Arlington, VA, March 20, 1995.

Department of Commerce, *Global Information Infrastructure: Agenda for Cooperation,* Washington DC, U.S. Government Printing Office, February 1995.

General Accounting Office, *Computer Security: Hackers Penetrate DoD Computer Systems,* GAO/IMTEC-92-*5,* U.S. Government Printing Office, Washington DC, November, 1991.

General Accounting Office, *Computer Security: Virus Highlights Need for Improved Internet Management,* GAO/IM-TEC-89-57, U.S. Government Printing Office, Washington DC, June, 1989.

General Accounting Office, *Export Controls: Issues in Removing Militarily Sensitive Items from the Munitions List,* GAO/NSIAD-93-67, U.S. Government Printing Office, Washington DC, March, 1993.

General Accounting Office, *IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information, GAO/AIMD-93-34,* U.S. Government Printing Office, Washington DC, September, 1993.

Information Infrastructure Task Force, *National Information Infrastructure Progress Report, September 1993-1994*, Department of Commerce, September 13, 1994.

Joint Security Commission, *Redefining Security; A Report to the Secretary of Defense and the Director of Central Intelligence*, U.S. Government Printing Office, Washington DC , 1994.

Marshall, Richard H. L. Lt. Col, USAF, NSA, Assistant General Counsel, Letter to Mr. Robert Rankin, SAIC, Serial: AGC(I)-027-95, Ft Meade, MD, 1995.

Munro, Neil, *The Quick and the Dead--Electronic Combat and Modern Warfare,* St, Martins Press, New York, 1991.

National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*, National Academy Press, Washington DC, 1989.

Naval War College, *Symposium Report: Evolving the National Information Infrastructure (NII); A Symposium for Government and Industry,* Naval War College, January 9, 1995

Office of Technology and Assessment, *Accessibility and Integrity of Networked Information Collections,* National Technical Information Service, August 1993.

Office of Technology Assessment, *Electronic Enterprises: Looking to the Future,* OTA-TCT-600, U.S. Government Printing Office, Washington DC, May, 1994.

Office of Technology Assessment, *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change,* OTA-TCT-527, U.S. Government Printing Office, Washington DC, May, 1992.

Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, U.S. Government Printing Office, Washington DC, 1994.

Office of the Federal Register, National Archives and Records Administration, *The United States Government Manual 1994/1995,* U.S. Government Printing Office, Washington DC, 1994.

Office of the Manager, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, An Awareness Document,* Arlington, VA, December 5, 1994.

Ruffin, Albert, Ed., *Federal Executive Directory,* Carroll Publishing Company, Washington DC, 1994.

Schwartau, Winn, *Information Warfare, Chaos on the Electronic Superhighway,* Thunder's Mouth Press, New York, 1994.

Stoll, Clifford, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* Random House, New York, 1992.

The Guide To American Law, West Publishing Company, New York, 1984.

Toffler, Alvin and Heidi, *War and Anti-War; Survival at the Dawn of the Twenty-first Century*, Little, Brown and Company, Boston.

This page intentionally left blank.

APPENDIX C

ACRONYMS

ACDA	Arms Control Disarmament Agency
ACS	Assistant Chief of Staff
ACSI	Assistant Chief of Staff for Intelligence
AFCSC	Air Force Cryptologic Support Center
AFIWC	Air Force Information Warfare Center
AG	Attorney General
AIA	Air Intelligence Agency
AID	Agency for International Development
AMC	Advisory Management Committee
ARPA	Advanced Research Projects Agency
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASSIST	Automated Systems Security and Incident Support Team
AT&T	AT&T Corporation
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATM	Automated Teller Machine
BA	Bank of America
BAA	Broad Area Announcement
BELLCORE	Bell Communications Research, Incorporated
Boeing	The Boeing Company
C&D	Cover and Deception
C2	Command and Control
C2W	Command and Control Warfare
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
CAC	Combined Arms Center
CASRIP	Center for Advanced ______
CAT	Committee on Applications and Technology
CCEP	Commercial COMSEC Endorsement Program
CCI	Controlled Cryptographic Item
CCL	Commerce Control List
CD	Combat Developments
CECOM	Communications-Electronics Command
CERT	Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CHIPS	Clearing House for Interbank Payments
CIA	Central Intelligence Agency

CIAC	Computer Incident Advisory Capability
CINC	Commander In Chief
CISS	Center for Information Systems Security
CJCS	Chairman, Joint Chiefs of Staff
CMC	Classification Management Committee
CMW	Compartmented Mode Workstation
CNA	Center for Naval Analyses
CNET	Chief, Naval Education and Training
CNO	Chief of Naval Operations
COAST	Computer Operation, Audit, and Security Technology
COMNAVSECGRU	Commander Naval Security Group
COMPUSEC	Computer Security
COMSAT	Communications Satellite Corporation
COMSEC	Communications Security
COP	Committee of Principals
CPSR	Computer Professionals for Social Responsibility
CSAF	Chief of Staff Air Force
CSC	Computer Sciences Corporation
CSE	Center for Security Evaluations (DCI)
CSL	Computer Systems Laboratory
CSSPAB	Computer System Security and Privacy Advisory Board
CSTC	Computer Security Technology Center
CSTO	Computer Systems Technology office
CT	Cryptologic Technician
CTSS	Computer and Telecommunications Staff
DAC/S	Deputy Assistant Chief of Staff
DASD(C3)	Deputy Assistant Secretary of Defense (C3)
DCI	Director of Central Intelligence
DDCI	Deputy Director of Central Intelligence
DEA	Drug Enforcement Administration
DepAg	Deputy Attorney General
DepSecCommerce	Deputy Secretary of Commerce
DepSecNon-DefAg	Deputy Secretary of State, Non-Defense Agencies
DepSecState	Deputy Secretary of State
DEPSECDEF	Deputy Secretary of Defense
DES	Digital Encryption Standard
DHHS	Department of Health and Human Services
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIRNSA	Director of National Security Agency
DISA	Defense Information Systems Agency
DISSP	Defense-Wide Information Systems Security Program
DIW	Defensive Information Warfare
DMRD	Defense Management Review Decision
DMS	Defense Message System

DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DoEd	Department of Education
DoI	Department of the Interior
DoJ	Department of Justice
DOJIRS	DoJ Incident Response Service
DoS	Department of State
DoT	Department of Transportation
DoTreas	Department of Treasury
DP	Data Processor
DPA	Delegation of Procurement Authority
DPG	Defense Planning Guidance
DSS	Digital Signature Standard
DVA	Department of Veteran's Affairs
EAR	Export Administration Regulations
ECPMO	Electronic Commerce Program management Office
EDS	Electronic Data Systems Corporation
EFF	Electronic Frontier Foundation
EIPC	Electronic Privacy Information Center
EMP	Electromagnetic Pulse
EO	Executive Order
EOP	Executive Office of the President
ESC	Electronics Systems Center
ESNet	Energy Sciences Network
et seq.	Et sequentes--and the following
EW	Electronic Warfare
FAA	Federal Aviation Administration
FACSPMF	Federal Agency Computer Security Program manager's Forum
FAS	Foreign Agricultural Service
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEDCAC	Federal Computer Acquisition Center
FEDSIM	Federal System Integration and Management
FEMA	Federal Emergency Management Agency
FIPSPUBS	Federal Information Processing Standards Publications
FIRMRS	Federal Information Resources Management Regulations
FIRST	Forum of Incident Response and Security Teams
FISSP	Federal Information System Support Program
FIWC	Fleet Information Warfare Center
FNC	Federal Network Council
FPC	Facilities Protection Committee
FR	Federal Register
FRS	Federal Reserve Service
FTC	Federal Trade Commission

FTP	File Transfer Protocol
FTS2000	Federal Telecommunications System 2000
GAO	General Accounting Office
GII	Global Information Infrastructure
GITS	Government Information Technology Service
GPS	Global Positioning System
GSA	General Services Administration
GSII	Government Services Information Infrastructure
GSSP	Generally-accepted Systems Security Principles
GTE	GTE Corporation
HHS	Department of Health and Human Services
HPCC	High Performance Computing and Communications
HQMC	Headquarters, Marine Corps
HTCIA	High Technology Crime Investigative Association
I4	International Information Integrity Institute
IBM	International Business Machines Corporation
ICC	Interstate Commerce Commission
ICCIP	Inter-Center Council on Information Processing
ICCITS	Inter-Center Council on Information Technology Security
ICCN	Inter-Center Council on Networking
IDA	Institute for Defense Analyses
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IITF	Information Infrastructure Task Force
IMPWG	Information Policy Working Group
INFOSEC	Information Systems Security
INSCOM	Intelligence and Security Command
INTERPOL	International Criminal Police Organization
IO	Information Operations
IOSS	Interagency OPSEC Support Staff
IPC	Information Policy Committee
IPRWG	Intellectual Property Rights Working Group
IRM	Information Resources Management
IRMAC	Information Resource Management Advisory Committee
IRMC	Information Resources Management College
IRS	Internal Revenue Service
IRTF	Internet Research Task Force
IS	Intelligence Specialist
ISAT	Information Science and Technology
ISC	Information Systems Command
ISDN	Integrated Services Digital Network
ISMO	Information Security management Office
ISOO	Information Security Oversight Office
ISSA	Information Systems Security Association
ISSAA	Information Systems and Software Acquisition Agency

ISSC	Information Systems Security Committee
IT	Information Technology
ITA	Intermodel Transportation Agency
ITAR	International Traffic in Arms Regulation
ITMSC	Information Technology Management Council
ITS	Information Technology Service
ITSD	Information Technology Services Directorate
ITT	ITT Corporation
IW	Information Warfare
IWEB	Information Warfare Executive Board
JCS	Joint Chiefs of Staff
JSC	Joint Security Commission
KAPP	Key Asset Protection Program
LANL	Los Alamos National Laboratory
LEAF	Law Enforcement Access Field
LIWA	Land Information Warfare Activity
LLNL	Lawrence Livermore National Laboratory
Loral	Loral Corporation
MARCO	Marine Corps
MCCDC	Marine Corps Combat Development Command
MCI	MCI Communications Corporation
MFS	MFS Communications Company, Incorporated
MI	Military Intelligence
MILSATCOM	Military Satellite Communications
MISSI	Multilevel Information Systems Security Initiative
MOE	Measure of Effectiveness
MOP	Memorandum of Policy
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
NACSEM	National Communications Security Emanations Memoranda
NACSI	National Communications Security Instruction
NACSIM	National Communications Security Information Memoranda
NADIR	Network Anomaly Detection Intrusion Reporter
NASA	National Aeronautics and Space Administration
NCA	National Command Authority
NCC	National Coordinating Center
NCS	National Communications System
NCSC	National Computer Security Center
NDP	Navy Doctrine Publication
NDU	National Defense University
NEC	National Economic Council
NII	National Information Infrastructure
NIITF	National Information Infrastructure Task Force
NIST	National Institute of Standards and Technology
NIWA	Naval Information Warfare Activity

NRaD	Naval Research and Development Command
NRC	Network Reliability Council
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NRSC	Network Reliability Steering Committee
NS/EP	National Security/Emergency Preparedness
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Directive
NSDD	National Security Decision Directive
NSG	Naval Security Group
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Board
NSTC	National Science and Technology Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTI	Northern Telecom Incorporated
NTIA	National Telecommunications and Information Administration
NTISSC	National Telecommunications and Information Systems Security Committee
NTISSP	National Security Telecommunications and Information Systems Security Publication
NWC	Naval War College
OASA	Office of the Assistant Secretary of the Army
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ODCSINT	Office of the Deputy Chief of Staff for Intelligence
ODCSOPS	Office of the Deputy Chief of Staff for Operations
ODISC4	Office of the Director of InformationSystems for C4
OECD	Organization for Economic Cooperation and Development
OIS	Office of Information Security
OIW	Offensive Information Warfare
OMB	Office of Management and Budget
OMNCS	Office of the Manger, National Communications System
OPM	Office of Personnel Management
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the CNO Instruction
OPSEC	Operations Security
OS	Operations Specialist
OSD	Office of the Secretary of Defense
OSTP	Office of Science and Technology Policy
OSWR	Office of Science and Weapons Research
OTA	Office of Technology Assessment
OTCIXS	
PCAST	President's Committee of Advisors on Science and Technology

PCERT	Pursue Computer Emergency Response Team
PDD	Presidential Decision Directive
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIC	Policy Integration Committee
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PM	Program Manager
POC	Point of Contact
POM	Program Objective Memorandum
PRD	Presidential Review Decision
PSC	Personnel Security Committee
PSN	Public Switched Network
PsyOps	Psychological Operations
PTI	Pacific Telecom, Incorporated
R&D	Research and Development
RDA	Research, Development, and Acquisition
RM	Radioman
RSA	Rivert, Shamir, Adleman
RVWG	Reliability and Vulnerability Working Group
S&T	Science and Technology
SARDA	(Assistant) Secretary of the Army for Research, Development, and Acquisition
SATAN	Security Administrator's Tool for Analyzing Networks
SC	Assistant Chief of Staff for C4 (Office Code)
SEALS	Sea Air Land (Special Operations)
SECDEF	Secretary of Defense
SIF	Security Issues Forum
SIGINT	Signals Intelligence
SISS	Subcommittee on Information Systems Security
SIWS	School of Information Warfare and Strategy
SOCS	Subcommittee on Computer Security
SONET	Synchronous Optical Network
SOPs	Standard Operating Procedures
SPB	U.S. Security Policy Board
SSA	Social Security Administration
STS	Subcommittee on Telecommunications Security
TIIAP	Telecommunications and Information Infrastructure Assistance Program
TIS	Trusted Information Systems, Inc.
TPC	Telecommunications Policy Committee
TPDC	Training and Professional Development Committee
TRADOC	US Army Training and Doctrine Command
TRADOC	Training and Doctrine Command
TRANSCOM	U.S. Transportation Command

TRW	TRW Incorporated
U.S.	United States
U.S. West	U.S. West Incorporated
UCC	Uniform Commercial Code
UNISYS	UNISYS Corporation
UnSecEnergy	Under Secretary of Energy
USA	United States Army
USAF	United States Air Force
USCG	United States Coast Guard
USD(A&T)	Undersecretary of Defense for Acquisition and Technology
USD(P)	Undersecretary of Defense for Policy
USDA	U.S. Department of Agriculture
USIA	United States Information Agency
USMC	United States Marine Corps
USN	United States Navy
USNPGS	U.S. Naval Post-Graduate School
USPS	United States Postal Service
USSS	United States Secret Service
USTA	United States Telephone Association
VCJCS	Vice Chairman, Joint Chiefs of Staff
WG	Working Group
WGET	Working Group on Encryption and Telecommunications
WILTEL	Williams Telecommunications Group Incorporated
XIWT	Cross Industry Working Team
XO	Deputy Chief of Staff for Operations (Office Code)
XOX	Assistant Deputy Chief of Staff for Operations (Office Code)